


3 1761 11648448 6



Digitized by the Internet Archive
in 2023 with funding from
University of Toronto

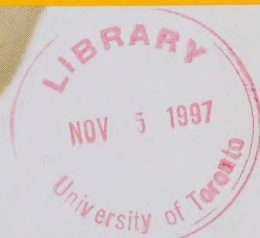
<https://archive.org/details/31761116484486>

CAI
PC
- A57

61372 32057

PRIVACY COMMISSIONER

ANNUAL REPORT 1996-1997



Annual Report Privacy Commissioner 1996-97



The Privacy Commissioner of Canada
112 Kent Street
Ottawa, Ontario
K1A 1H3

(613) 995-2410, 1-800-267-0441
Fax (613) 947-6850
TDD (613) 992-9190

© Canada Communications Group
Cat. No. IP 30-1/1997
ISBN 0-662-63040-8

This publication is available on audio cassette, computer diskette and on the Office's Internet home page at <http://infoweb.magi.com/~privcan/>



Privacy
Commissioner
of Canada

Commissaire
à la protection de
la vie privée du Canada

The Honourable Gildas L. Molgat
The Speaker
The Senate
Ottawa

July 1997

Dear Mr. Molgat:

I have the honour to submit to Parliament my annual report which covers the period from April 1, 1996 to March 31, 1997.

Yours sincerely,

Bruce Phillips
Privacy Commissioner





Privacy
Commissioner
of Canada

Commissaire
à la protection de
la vie privée du Canada

The Honourable Gilbert Parent
The Speaker
The House of Commons
Ottawa

July 1997

Dear Mr. Parent:

I have the honour to submit to Parliament my annual report which covers the period from April 1, 1996 to March 31, 1997.

Yours sincerely,

A handwritten signature in cursive script that reads "Bruce Phillips".

Bruce Phillips
Privacy Commissioner

The Year at a Glance

April 1996

- Appearance before House of Commons Transport Committee on Bill C-20, privatization of Air Navigation System (page 33)
- Canada Post photocopying competing courier mail (page 45)
- Commissioner responds to Solicitor General's DNA databanking paper (page 24)

May

- Canadian Privacy Commissioners meeting, Victoria, B.C.
- Health Canada files found in Winnipeg dumpster (page 46)
- Information Highway Advisory Council report calls for framework privacy legislation by the year 2000
- CDMA endorses government plan for private sector law

June

- Census Day
- House of Commons Committee on Human Rights and Status of Persons with Disabilities Roundtable on privacy and new technologies (page 29)
- Appearance before Senate Committee on Transportation & Communications on privatization of Air Navigation System
- Cabinet orders local telephone companies to make customer databases available to competing directory publishers (page 37)
- Appearance before House of Commons Justice and Legal Affairs Committee on operations
- Pilot match begins of all returning air travellers' customs declarations with employment insurance database (page 7)

July

- CRTC licences first Personal Communications Systems (page 38)

August

- Uniform Law Advisory Group on Protection of Personal Information considers comprehensive data protection law
- Federal Court rules against access to Canada Labour Relations Board members' notes (page 40)

September

- Justice Minister commits Canada to private sector privacy law at 18th International Privacy and Data Protection Commissioners Conference, Ottawa (page 76)
- Appearance before House of Commons Finance Committee on review of financial institutions White Paper
- Ontario Human Rights Board of Inquiry rules major corporation's substance testing program unlawful

October

- Appearance before Standing Committee on Procedure and House Affairs on permanent voters list (page 19)
- First complaints against Customs-HRDC match
- Tax audit documents found in cabinet bought at government surplus store (page 44)

November

- Appearance before Select Committee on Law Amendments, New Brunswick Legislature on proposed privacy bill
- Canada Post debiting credit cards for unordered merchandise (page 45)

December

- CRTC announces hearings on costs of unlisted phone numbers (page 38)

January 1997

- HRDC asks Office to review Labour Market Initiatives with Indian Bands

February

- Appearance before Special Joint Committee on a Code of Conduct for MPs
- National Forum on Health final report calls for national health information database (see page 14)
- Appearance before Sub-committee on *Firearms Act* regulations (page 21)

March

- Human Rights Committee holds cross-country hearings on privacy and technology
- Reported to Transport Canada on Air Navigation System files (page 49)

Table of Contents

On the One Hand...	1
...On the Other	3
Nothing to Hide—and Nothing to Prove	7
One Stop Shopping—The Common Client Identifier	11
A National Health Database	14
Population Registers	19
The Permanent Voters Register	19
The Firearms Registry	21
DNA Databanking	24
Where Should Parliament Draw the Line?	29
Privatization and Devolution: Who's in, who's out?	32
Publicizing the Identity of High-Risk Offenders—an update	35
This Year's Telecommunications News	37
In the Courts	40
Incidents	42
Audits	47
Notifying the Commissioner	51
Investigations Branch	54
Cases	55
Inquiries	66
International Privacy Commissioners Meet in Ottawa	74
Privacy Protection In Canada...an update	76
Corporate Management	79
Organization Chart	81

On the One Hand...

Paradox. (*n.*) *person or thing having contradictory qualities.*

— The Oxford Dictionary.

The 'thing' in this case is the Government of Canada. Paradox perfectly describes the contradictory and confusing behaviour demonstrated in the last year in the field of privacy rights. Some of the most hopeful and encouraging developments in a decade have run parallel with some of the most disturbing and dangerous.

We have seen both a growing recognition of the pressing need for stronger and more comprehensive laws to protect Canadians' privacy rights—and we have witnessed actions which threaten to make a shambles of those rights. Which will triumph?

Thumbs up

On the positive side, nothing equals in importance Justice Minister Allan Rock's pledge that, by the year 2000, there will be federal law to provide "effective, enforceable protection of privacy rights in the private sector". The government recognizes that technology has made it all but impossible to maintain effective privacy protection without covering both the public and private sectors.

This Office has long advocated such a step. And it has the endorsement of the government's own Information Highway Advisory Council, the Canadian Direct Marketing Association, the Information and Privacy Commissioners of Quebec, Ontario and British Columbia, to mention only a few. Let us hope that some vestiges of our privacy remain to be protected by the millennium.

Curiously, the Minister's announcement drew only passing mention in the media. I say 'curiously', given the generally first-class record of Canadian media in keeping abreast of privacy issues, and because this was the most significant statement of government privacy policy since the passage of the *Privacy Act* itself in 1983.

Similarly overlooked was a landmark study by the House of Commons Standing Committee on Human Rights chaired by the Hon. Sheila Finestone. This committee devoted the better part of a year to the study of privacy rights and new technologies, visiting several cities and hearing from scores of witnesses representing every shade of opinion.

In April, as the House was rising for the election, the committee released its report, *Privacy: Where do we Draw the Line?* The report is nothing less than breathtaking both in its scope and depth. What distinguishes it from earlier reports is its recognition of privacy's fundamental value to Canadian society and not a "token to be bartered for social and economic benefits". One committee member describes privacy as an "associative" right—one that is essential to free association, free speech, and to our very autonomy. The report offers a guide for grappling with one social and ethical impact of the new technologies.

Mr. Rock could do no better than to merge this committee's work with that of the Information Highway Advisory Council (which focuses on the consumer and business case for privacy on-line) and the Canadian Standards Association's model privacy code as the outline for his promised new privacy law.

The document deserves far more than the scant public attention it received. As the movie critics say, Two Thumbs Up!

Another important Parliamentary development was the Commons' unanimous endorsement of a private member's motion (Mr. Paul Crête, Kamouraska, Rivière-du-Loup) to extend the existing *Privacy Act* to cover all Crown corporations, a step advocated both by this Office on more than one occasion, and by the Commons Justice Committee in its 1987 review of the *Privacy Act*. Here was a clear expression by all parties in the House which, although not law, is both a strong direction to the government and clear indication of Members' growing awareness of the rising public concern over privacy intrusions.

The government also has responded at last to our repeated pleas to stop the erosion of privacy rights as it prunes its bottom line. Transforming government operations into an array of not-for-profit bodies, commercialized monopolies and competitive companies was depriving their clients and employees of legally established privacy rights.

After some hesitation, during which air traffic control operations were transferred to a private company (NAV CANADA) absent those rights, a new policy is promised which will continue *Privacy Act* protection for newly privatized agencies. We applaud the promise and anticipate its arrival.

Finally, we welcome the growing practice among government departments to seek our comment and advice on specific proposals or plans which have privacy implications. Our last report drew attention to a successful collaboration with the Chief Electoral Officer to ensure protection and respect for Canadians' privacy rights in the new permanent electronic voters register.

Other major information users too, Statistics Canada and Human Resources Development Canada (HRDC) among them, have sought our input in major undertakings. HRDC, in particular, is examining several projects, one of which—a common client identifier akin to a universal identification number—literally bristles with privacy implications. Some of these proposals represent a major test of the theory that technology and privacy can co-exist. We will follow them with care and concern.

Government departments are not obliged to consult the Privacy Commissioner. But it is hard to conceive of a more useful application of staff expertise and insights than helping government departments achieve their policy and management objectives in ways that respect the rights of Canadians. Mrs. Finestone's committee recognized the value of this consultative function and recommended making it part of the Office's official mandate.

If the tale could end here, the year would have been one marked by steady progress. But life seldom proceeds so smoothly.

...On the Other

Attention now turns to a practice which poses a deadly threat to privacy and to its corollary—autonomy and personal freedom. It has led us into a head-on collision with two great departments of government, HRDC and Revenue Canada, precipitating a legal challenge which may ultimately determine whether privacy is a fundamental value of this society or merely an irritant quickly to be consigned to the scrap heap of unfulfilled good intentions when the going gets tough.

That issue is data matching, an innocent-sounding activity with the capacity to demolish any real right to privacy and certainly to destroy the basis of trust which must exist between citizens who provide, and governments which collect, personal information.

Given the intense pressure on government departments to be leaner (and, if necessary, meaner) coupled with the alluring ease of tracking citizens with computers, a confrontation was probably inevitable.

At issue is HRDC's practice of collecting data from the Customs declarations of every returning air traveller to identify employment insurance claimants who were out of the country while receiving benefits. EI claimants must report any extended absence from their normal residence for the good reason that they are expected to be looking, and available, for work. HRDC officials (and many

taxpayers) have long been troubled by anecdotal evidence—approaching an urban legend—that many claimants were enjoying holidays at taxpayers' expense. The department's administration and enforcement methods were allegedly proving ineffective.

HRDC conceived the notion of matching the EI data base with that of returning travellers customs declarations. The match would quickly show whether any of those millions were receiving employment insurance payments. It would then be a simple matter to find whether they had reported their absences.

Doubtless such a match will catch some who may be cheating EI. But the price it exacts is far too high. It systematically searches millions of innocent travellers, without their knowledge or consent, who filed customs returns on the assumption—and on Revenue Canada's word—that they would be used for customs purposes only.

The match offends the most fundamental principle of any privacy law; that government tell its citizens why it is collecting personal information, then use it only for that—and not a wholly unrelated—purpose (unless the individual consents). The reason for the principle is clear: to prevent the government from conducting unwarranted surveillance on its citizens by prowling through its immense personal databanks on what amounts to nothing more than high-tech fishing expeditions.

Let us try a pre-computer age analogy. Assume there are some criminals at large in your community. Assume that the police therefore embark on a search of every single household, without warrant, without notice, without permission, and without any cause to suspect any particular household. The police just show up, barge through the door, and look around. How long would any community accept such arbitrary behaviour?

Yet, in an information context, that is precisely what data matching makes possible—a systematic search of everyone. Governments which match data this way have turned the presumption of innocence on its head; everyone is suspect until the computer proves them innocent. It is akin to what an earlier privacy commissioner described as “high technology search and seizure”. If we allow government to carry on in this fashion, they will routinely scrutinize every record of every citizen until they unearth some evidence of guilt.

A privacy commissioner cannot accept a data search that ignores the presumption of innocence, the need to identify some reasonable grounds for suspicion, and the absence of independent authorization. If such matches become standard practice,

we face virtually open season on any personal information we entrust, or are forced to deliver, to government.

Unable to convince bureaucrats, or their ministers, to modify the match, we sought legal advice from one of Canada's leading constitutional experts. His advice buttressed our position that the data match violates the search and seizure provisions of the *Canadian Charter of Rights and Freedoms*. We are currently exploring with the government the most expeditious manner of getting the matter before the Courts for resolution.

No more crucial issue has arisen in my six years in this Office. I have no more interest in protecting UI cheats from detection than the next taxpayer. I have every interest in preventing government from putting millions of law-abiding Canadians under "dataveillance". As a people and a society, we enjoy Charter protection against having to prove our innocence. One's Charter rights should not be compromised simply because technology makes it possible.

The premise of this match is boundless—once entrenched, we are on the slippery slope to a general surveillance system in which personal data from all levels of government are routinely shared and matched.

A recent letter from Mr. Whyte of Toronto, argues that the practice "opens the door to abuse of information power of government" and urges citizens to resist. While this match may seem "reasonable and popular", he argues that it could establish a precedent for government to use customs information "to determine which citizens have travelled to a country whose policies they may oppose, whose trade they may wish to restrict, or for any other purpose.... Travel information is routinely used by autocratic regimes to restrict and control their citizens. We must not allow this precedent to be established in Canada. This match must be resisted as a routine protection of our liberty. I urge you to stop this misuse of customs information."

The Information "Panopticon"

In effect, such a match is an electronic version of late 18th century philosopher Jeremy Bentham's Panopticon. Bentham proposed a design for a prison which would allow guards to observe prisoners from a central tower from which they could see out but no-one could see in. The tower might, or might not, be occupied but the effect of his design was to create "a state of conscious and permanent visibility that assures the automatic functioning of power". Effective but chilling.

Technology now furnishes government with the power to create an information Panopticon. Why should it not seize the advantage? Perhaps we would all

behave impeccably—or, at least, differently—if we thought someone might observe our every transaction. There is no underestimating the power of fear and embarrassment for social control—hence the loss of our autonomy. But we must not concede to the bureaucrats that our society is so manifestly corrupt that we must subordinate our rights of individual autonomy and privacy to their interests in efficiency.

Well, you say, I have nothing to hide so what does it matter? Sometimes an individual's right has to give way to the interests of society as a whole.

Perhaps that is where we are losing our way. It's time to consider the damage that the unfettered exercise of power can inflict on our society. By concentrating on privacy as an individual right, we then are forced to play the game of "this right trumps that one—my right as a taxpayer not to be ripped off trumps your right not to be under surveillance".

It may be time to consider the view, espoused by Priscilla Regan in her book *Legislating Privacy*, that considering privacy as an individual right does not serve a strong basis on which to develop public policy. We should consider privacy's social importance; its inherent place as a bedrock value in a democratic society and understand how it influences our relationships with one another, with social, political and economic organizations, and what powers we are prepared to grant these organizations.

Protecting our privacy is not simply a matter of debating the value of an individual's self-interest versus a competing interest. Privacy also serves a common, public and collective interest. The value strengthens our society by reinforcing our sense of connection through mutual respect.

Whatever we do to protect privacy, we must recognize the import of the value and the consequences to our liberty if we are lazy enough—and short-sighted enough—to consider it an administrative nuisance that gets in the way of efficiency and the bottom line. This is the path to the Surveillance Society. I urge the government not to take it.

A handwritten signature in dark ink, reading "Bruce Phillips". The signature is written in a cursive, flowing style with a large, prominent 'B' and 'P'.

Nothing to Hide—and Nothing to Prove

Characterizing the options governments are now considering as the path to a surveillance society is far from overstatement. Granted Canadians view governments generally as benign—part of our fortunate heritage. Geography and climate require our governments to have a social conscience, reflected in our social safety net. But funding and benefitting from that safety net do not mean abdicating our civic responsibilities, one of which is to ensure that we do not sacrifice individual choice and personal liberty at the altar of efficient government.

Governments now have the means for tracking virtually all their residents' contacts with the state, assembling comprehensive data bases from that data and sharing it widely. And with the means come the pressures—downsize, rationalize and deliver service more efficiently. Some of this information collection is a legitimate activity of a government program—a "consistent use" of the data. Some, we find disturbing. And one, we argue—matching returning travellers customs declarations with the employment insurance database—is so broad as to be an unreasonable search and seizure under the Charter.

This year's report examines just a handful of the past year's developments: the Revenue Canada Customs/Employment Insurance match, proposals for a single cards, single numbers and comprehensive personal social program data to be shared among governments, a national electronic health database, and several population registries; the permanent voters list, the firearms registry and the DNA databank.

And there is also a hopeful note—the comprehensive and forceful report by the Parliamentary human rights committee on dealing with the impact of new technologies on privacy.

The Customs - Employment Insurance Data Match

Data matching links personal data from a variety of unrelated sources, virtually always in electronic form, to make administrative decisions about those using government programs and services. Since matching is an indirect—and usually invisible collection of data, the government has established a process to control the practice.

One of the steps is providing the Privacy Commissioner with a "preliminary feasibility study" 60 days before the match is to begin. This allows the Commissioner, as an Officer of Parliament, to act as an advocate for the individuals whose records are to be matched. The Office reviews the proposal

and makes any recommendations to the head of the department who is free to accept or ignore the comments. The Commissioner has no power to stop or alter the match.

This lack of power has caused little difficulty until now; departments have been sensitive to the issue and generally accepted the Office's recommendations. But the times, they are a-changing. The advent of bottom-line management has prompted a get-tough attitude in departments which provide substantial benefit payments. All to the good, most taxpayers would say. Not so good, we say, when a match is so broad it risks more than offending the *Privacy Act*; it threatens fundamental rights. Such a case, we argue, is the match of travellers' Customs declarations with employment insurance benefit files.

The practice at issue in this case is Human Resources Development Canada's (HRDC) match of data from Revenue Canada's *Travellers Declaration Card*, or Form E311, with records of Employment Insurance claimants to determine whether they had been out of the country while drawing benefits.

The Customs declaration All travellers entering Canada by common carriers (air, train and bus) must complete the card and give it to the customs and immigration official at the entry point. Travellers supply their name, address, date of birth, the airline and flight number, whether arriving from the U.S. or elsewhere, the last three countries visited on the trip, whether the travel was business or personal, the type of goods they are bringing into Canada, whether they will visit a farm in the next 14 days, the date of departure from Canada, the date of return, the value of the goods they purchased and the personal exemption claimed. A customs stamp identifies the airport.

Both departments approached the Office informally in June 1995 to discuss the proposed match. Given that the evidence of abuse was largely anecdotal, privacy staff asked the departments to provide some factual substantiation for the match, including a cost-benefit analysis.

There are four phases to the match: a feasibility study to gather data for a cost benefit analysis, a reprocessing of the feasibility study, a proposed six-month pilot project and, finally, a projected full implementation in late 1997.

The feasibility study In order to gather the data for a formal matching proposal, Revenue Canada and HRDC signed an agreement in June 1995 in which Revenue Canada would disclose traveller information to HRDC in order to conduct a feasibility study to detect potentially fraudulent EI claims.

The agreement provided for the disclosure of traveller cards to begin July 4, 1995. Revenue Canada would gather a sampling of traveller cards from nine airports for the months of June, September and November 1994 and February and March 1995. HRDC agreed not to take any enforcement measures against individuals identified through the matching process.

Since Revenue Canada stores traveller declarations on microfiche, HRDC agreed to pay staff, working on site at Revenue Canada, to convert the information from the 16,861 samples into electronic format and load it onto diskettes. The data included name, date of birth, postal code, periods of travel and the microfiche roll and frame numbers on which the E311 is stored.

The electronic match identified 257 individuals who were out of the country while receiving EI benefits, or 1.5 per cent of the sample. HRDC returned the diskettes to Revenue Canada and obtained a photocopy of the E311 cards of the 257 individuals identified to validate the results of the match.

The data matching proposal HRDC analyzed the results of the feasibility study and submitted a formal data matching proposal to the Office in January 1996. In a meeting to discuss the proposed pilot project, Privacy staff underlined the Office's concern about using retroactive data, the lack of notice to travellers about the unrelated use of Customs data during the pilot project, and the lack of a written agreement to cover the terms of the exchange. It was understood that all would be taken care of before the project was implemented. HRDC completed its data matching proposal at the end of February and the Office notified the department on March 19, 1996 that it would not object to its conducting the pilot project.

HRDC obtained again from Revenue Canada the data it had used during the feasibility study and simply reprocessed it to firm up the figures. In early July 1996, HRDC gave copies of each matched individual's EI claim record and E311 to the claimant's regional insurance representative. The regional office forwarded the information to the appropriate CEC which wrote to each claimant seeking an explanation for their travel while collecting EI benefits. Revenue Canada did not remove any of the irrelevant travel information from the E311 cards it gave HRDC.

The pilot project HRDC considered its reprocessing of the feasibility study hits as the first phase of the pilot project. The departments did not sign a memorandum of understanding for the pilot project until April 1997. At the conclusion of the pilot, HRDC is to decide whether it will make the match an ongoing practice. HRDC continues to pay the costs of equipment and

30 employees at Revenue Canada to create the electronic database. Revenue Canada now also discloses the purpose for the individual's travel.

Since then, Revenue Canada has provided HRDC with computer tapes each month containing traveller declarations of Canadian residents during the months of December 1992, January to June 1993, December 1994 and January to March 1995. Although the approved retention schedule for E-311 microfiche cards is two years, Revenue Canada has kept them since 1992 for no apparent customs purpose. Revenue Canada estimates that approximately 18 million visitors and returning residents enter Canada by air alone each year.

The resulting hits and claim files are sent to the Miramichi Investigations Centre for verification and follow up. HRDC has taken action on the hits from December 1994 onwards. Individuals are contacted and those unable to justify their absence must repay the benefits for the period of absence, plus a penalty.

The E311 cards used in the match included no public notice of the disclosure and use of customs information for detection of possible EI fraud. Nor has either HRDC or Revenue Canada "accounted publicly for the use and disclosure of personal information", as government matching policy requires. Revenue Canada has begun removing irrelevant travel details on the cards that are disclosed to HRDC in case where the claimant contests the recovery of EI benefits.

The Commissioner concluded that the breadth of the match and its implementation were excessive. When repeated correspondence and meetings, including with both ministers, could not resolve the disagreement, he sought legal advice.

The Commissioner is seeking the Federal Court's guidance on the question of whether searching every returning traveller on suspicion of defrauding EI offends the "unreasonable search and seizure" provisions (section 8) of the Charter.

One Stop Shopping—The Common Client Identifier

The past year has seen all levels of government examine new ways to improve their delivery of income security programs and to share their clients' personal information. The government believes, with some justification, that Canadians do not much care what level of government delivers the service as long as it is delivered.

However, the most immediate impact of different governments and agencies sharing clients' personal information and program delivery is that the information will be linked and shared among many users inside and among governments. Individuals will have even less control over their personal information and greater accessibility will almost inevitably increase the chances that the information will be used or shared inappropriately—for purposes other than those for which it was collected.

A second privacy concern is the need for a common method for all levels of government to identify or "authenticate" the client; thus a "common client identifier". Dependable personal identity is required at every step of the process, from applying for and delivery of financial benefits, linking to other programs and services, maintaining case files, controlling fraud and errors, and terminating benefits. Thus a common client identifier is considered critical. So too is a central database accessible to all income security programs and levels of government.

In effect, the proposals amount to comprehensive and systematic data matching on a scale never done before.

A group of information technology managers from the income security departments of the federal, provincial and territorial governments have been studying the issues. The group's recently-released report, *Enhanced Service Delivery Through a Common Client Identifier: Options and Opportunities*, suggests that using a common identifier (and its supporting database) could produce significant gains. It would properly identify legitimate claimants before the benefits are paid, rather than matching data after the fact to detect fraud, then attempting to recover improper payments.

The report identifies several important features of an effective common identifier. These include the need for it to be used in all jurisdictions, unique to the individual, applicable to all benefit programs, and secure against forgery or

tampering. The common client identifier must also protect privacy and result in minimal intrusion into clients' lives. Among the options the group considered for a common client identifier were:

- the status quo (name/birth date)
- the current Social Insurance Number (SIN)
- a "modernized" SIN (including positive client identification, such as a PIN) and establishing the SIN Register as a central database which would identify every individual in all income security programs)
- a "new" number to act as a common identifier for all federal/provincial/territorial income security programs
- the provincial health care number.

The working group seems to favour either a modernized SIN (with the existing SIN acting as a transitional Common Client Identifier) or a new number created specifically as the common identifier. The notion of using provincial health cards and any "biometric" features (such as digitized fingerprints) seems to have been rejected for now.

Although we are prepared to keep an open mind on many aspects of the group's work, any proposal that builds on the existing SIN is in for heavy weather. Never was a personal identifier so compromised. While the federal government has a restrictive policy on its own uses (since 1989) SINs are everywhere—landlords, credit bureaus, libraries, video stores, supermarkets—the shorter list is who does not have them. Constructing a common client identifier on the SIN is building on sand.

The working group acknowledges that among the barriers to success are public concerns about individual privacy and confidentiality, restrictions against sharing and disclosure in both privacy and program legislation and legislative restrictions on the use of the SIN. In fact the report identifies the perceived impact on privacy as the single greatest barrier to the development of a common identifier.

In this respect, the report is right. While more efficient delivery of government services is a noble goal, in its pursuit we may well demolish the walls so carefully constructed around personal data files. These walls prevent governments from assembling comprehensive personal profiles of their citizens and from using information collected for one purpose for a totally unrelated purpose. Protecting privacy in this context requires, to paraphrase an American Supreme Court decision, "[protecting] the fragile values of a vulnerable citizenry from the

overbearing concern for efficiency that may characterize praise-worthy government officials no less, and perhaps more, than mediocre ones."

Government must address several matters before accepting the concept of a common client identifier: First, there must be sound, proven justifications for pursuing such an identifier. To date, there has been a noticeable lack of empirical evidence supporting its introduction. There is no lack of desire to find a quick fix by applying technology to social and economic problems, but the search for such solutions must not replace a hard-nosed analysis of their merits .

Second, if governments can demonstrate the need, then legislation must precede any development of a common client identifier. As Alberta Privacy Commissioner Robert Clark remarked, we cannot have the "technocrats stepping on the democrats". The uses of the identifier and privacy protection mechanisms must be specifically set out in legislation, and there must be stringent penalties for misuse of the system.

Finally, the impact of introducing a common client identifier must be fully understood before any implementation. Both a privacy impact assessment and a broader societal impact assessment should be completed. While the report has no official endorsement, it will likely form the basis for Human Resources Development Canada to develop a business case for a common identifier in income security programs.

The Privacy Commissioner has agreed to comment on the substantial privacy impact of the project with the usual caveat; he cannot give seals of approval. The Commissioner must guard his independence in order to be a credible and unbiased investigator of any complaints.

The federal Privacy Commissioner is not the only one concerned about this issue. Provincial and territorial commissioners too are watching warily. The Office has agreed to gather and share information and co-ordinate the response of privacy commissioners.

A National Health Database

The National Forum on Health, a panel of health experts, was established by the Prime Minister in 1994 to "involve and inform" Canadians about health care issues. The Forum was also to advise the federal government on ways to improve Canadians' health and the health care system. Among the Forum's recommendations in its 1997 final report, *Canada Health Action: Building on the Legacy*, are several on the need for better information or "appropriate, balanced and high-quality evidence" to improve health care decisions. In the terminology of the profession, this is "evidence-based" medicine.

Specifically, the Forum recommends exploring the role information technology could play in setting up a national health data network. The 1997 federal budget set aside \$50 million for a Canadian Health Information System to include a national health surveillance network, a population health clearinghouse and a First Nations health information system.

The Forum also proposes that provincial and territorial agencies develop and maintain a standardized set of longitudinal data to chart changes in individuals' health status over time.

And, finally, the Forum suggests that collecting and integrating all 'Canadians' health data is not enough; a person's health is influenced by a number of factors, many of them non-medical. Thus, the forum is interested in studying the relationship between health and social status, and how social and economic factors such as poverty, unemployment and cuts in social support affect individual's health. The Forum advocates linking clinical and administrative health data with such non-medical information as income, employment and educational status. However, it wishes to exempt health research from the normal obligations of privacy laws—such as obtaining the patients' consent for use of their personal information, destruction of the data on approved schedules, and obtaining the patient's authorization for further disclosures.

In summary, the Forum's recommendations foster an accelerated government drive for access to patient information in the hope of better controlling and managing the delivery of health care services. The recommendations also advance the notion that the research community should have access to the records of the entire Canadian population, yet should be exempt from privacy laws governing access to, and use of, that data. And, finally, in the interests of efficient care and research, it further proposes to computerize all these files to improve the flow of information across all jurisdictions.

While we cannot assess the claimed superiority of evidence-based medicine, we can say that adopting an evidence-based system is potentially one of the most significant privacy issues of the decade for Canadians. It represents a revolution in the way health information is collected, disseminated and used because it relies on state-of-the-art information technology to integrate information from all health sectors—for example, doctors, hospitals and pharmacists. It also envisages amalgamating health information with socio-economic data such as education and income. And it recommends that not just health care providers, but all health administrators and policy makers, have access to the information to make decisions about health care. Information about specific individuals, not aggregate data, is one of the key requirements for developing such a system.

It is hard to argue with any proposal to make better-informed health care decisions. Privacy advocates want effective health care as much the next Canadian. We also recognize that broader research may enhance our understanding of the factors affecting our health and improve delivery of health services.

However, using personal health information to foster an improved health care system is not a purely a win-win scenario. The Forum's proposals pose significant challenges to the privacy of Canadians' medical records—the right to protect the confidentiality of that personal information, and the right to be informed of, and consent to, all other uses of that information. The prospect of greatly expanded collection and sharing of personal medical information sets privacy alarms ringing.

Traditionally privacy laws and medical ethics have allowed only those directly involved in patient care to have access to patient medical records. Medical ethics and legal prohibitions exact a high standard of care and protection for the confidentiality of medical records. With few exceptions, the right to control the flow of one's personal medical information rests with the patient, not the physician, nor the hospital, nor the state.

An information network to support evidence-based health care would turn that important centuries-old rule on its head. Medical records, currently accessible to patients and a limited number of others, could no longer be said to be confidential when hundreds of strangers can access them electronically.

The experience south of our border merits mention. American law professors Paul Schwartz and Joel Reidenberg cite an observation in a U.S. medical journal that "medicine is increasingly a spectator sport." Say Schwartz and Reidenberg, "A widening audience of outside observers now watch the performance of

doctors, nurses and patients, and personal data plays a critical role in the evaluation of their behaviour."

Canadians may argue that our health care system is different—that the strong government component in our health care system makes the information in the system less vulnerable to abuse. We argue that it is precisely because the state has such an important role in delivering health care that there must be mechanisms for the individual to counter that power and exert some control. While Canadians tend to view government as largely benign, that should not mean abdicating individual consent and responsibility.

As well, our system is becoming increasingly privatized; services such as home care, speech pathology and various types of testing are now performed by private companies. And now with the advent of drug plans, pharmacies (which have always been private) deal frequently with private insurance companies and do so increasingly on-line. We will see the same pressures that now exist in the U.S. to use medical information for purposes that have nothing to do with the health of the patient or even the good of society. Personal health information will become an ever more valuable commodity in the data marketplace.

Canada must not seize upon evidence-based health as a medical nirvana without sober reflection on the impact this massive assembly of personal information—health and other—may have on our privacy and autonomy.

Some Canadians may not object to substantially diminishing the confidentiality of their medical records. But the freedom to decide whether to participate in such a wide-ranging scheme is an essential component of privacy protection and democracy, and must be preserved. To protect those who object, any health network must allow individuals to prevent their medical information from being stored and accessible on this network. And people who choose not to participate should not be penalized by receiving a lesser standard of health care.

It is essential to get a grip on the issues involved in preserving the privacy of health care information. Among the measures we propose are the following:

- Enact complementary federal and provincial legislation to protect the privacy of the full range of personally identifiable health care information. The legislation would incorporate the fair information principles of international data protection agreements. This must be done before the health network develops further.
- Establish clear requirements for obtaining the informed consent of patients to disclosures of personal information. In the absence of informed consent, an individual's right to control the disclosure of personal medical information

should be paramount. That right should be overruled only in the face of an overwhelming and compelling public interest (or to provide the patient emergency care). Conducting research does not always constitute an overwhelming or compelling public interest.

- Establish strict limits and controls on the circumstances under which access to personally-identifiable information is granted to secondary users for research purposes and encourage the conduct of research through the use of aggregate, de-personalized data.
- Establish strong remedies in law for disclosing information without a patient's consent.
- Educate patients about how their records are used and the privacy implications of having their medical records computerized and placed on a national network.
- Develop guidelines to address the privacy and security issues raised by the computerization of patient data, including provisions for full audit and control.
- Establish an independent review mechanism to oversee the privacy of health care information.

If medical records are linked to employment, educational and other socioeconomic databases, they would reveal not just medical information but whole life histories. For the medical community, this may be the point. But, easy as it is to rationalize data gathering as beneficial for the individual and society, the information might not be used for benevolent purposes. The collection of medical data can slide imperceptibly from health care to medical supervision to lifestyle surveillance and, ultimately, to a more generalized form of surveillance by the state.

For this reason, it is critically important that we examine how to prevent further secondary uses of this information, such as by law enforcement agencies, employers and private individuals (such widespread uses are almost the norm in the United States). The purpose of those databases must be limited to advancing health care, and nothing else. They must not be allowed to become a convenient means for government agencies and private businesses to conduct non-medical surveillance of citizens who are simply making use of an essential service.

Of course, there is a balance of interests to be weighed between the two poles of better personal and societal health, and individual autonomy. And we acknowledge the potential beneficial uses of health information and the importance of research. There are important differences between using personal

data and aggregate data, stripped of personal identifiers. But we insist that protecting the privacy and confidentiality of individual health information is also critical to open communication between medical personnel and patient, and patients' trust in the system. Protecting privacy deserves as high a priority as improving health systems.

The Final Report of the National Forum on Health recognizes the importance of privacy in developing a national health information system. And the federal health department intends to address privacy in its planning of such a system and we hope to assist this critical work. But a Canadian health information system could either stand or fall on the extent to which it incorporates privacy, patient autonomy and informed consent. How well privacy fares in the development of this system may well determine whether the public will be willing participants—or will mount the barricades to protest against the extraordinary level of surveillance it makes possible.

We look forward to legislative guarantees that the system will protect rather than jeopardize individual health information.

Correction: Last year's annual report expressed concern about the lack of legal protection for data in a national longitudinal health survey being conducted by the Canadian Institute for Health Information. In fact, the survey is being conducted by Statistics Canada under the authority (and protection) of the *Statistics Act*. We apologize for the error.

Population Registers

The perennial challenge of population registers for a privacy ombudsman is where to draw the line between pragmatic acceptance of lists assembled for administrative purposes (but with solid privacy protection) and a healthy sense of unease at the growing pressures to identify and quantify citizens in various electronic databases. Once in a database it is but a small step to comprehensive profiles, all in the name of greater efficiency.

The Office followed the creation of several registers this year with varying degrees of concern; the permanent voters register, the firearms registry and the proposed DNA data bank.

The Permanent Voters Register

On April 10, 1997, federal enumerators began going door-to-door for the last time. Information collected from this final, in-person enumeration will form a permanent electronic register of electors. The register is the culmination of several years of work for Elections Canada. From now on, lists for federal elections—and, potentially, for provincial and municipal elections—will be drawn from the register which will be updated from other federal databases (with the voter's consent) and, eventually, from specified provincial data bases.

Although the idea of a permanent electronic voters register had been floated before, work began seriously at Elections Canada in 1994. Knowing the Commissioner's concern about building such a comprehensive electronic register of citizens, Elections Canada approached him to provide systematic input to the project as it progressed. The Commissioner agreed and assigned a staff member to contribute. The Office's emphasis during the exercise was on what information Canadians need to surrender in order to exercise their right to vote, and how best to protect that information in an electronic data base.

In October 1996, amendments to the *Elections Act* were tabled in the House of Commons and the Commissioner was asked to appear to comment on the privacy implications. The amendments responded to most of his recommendations appearing in the 1995-96 annual report (*A Vote for Privacy?* page 14).

Other uses of the register The greatest worry with this type of register is that government will be tempted to use it for unrelated purposes. With growing budget pressures, and the electronic means at their disposal, bureaucrats increasingly view any personal data as fair game for any purpose—the "why

should you care if you have nothing to hide?" school of administration. The Commissioner sought legislative guarantees that the register would not be available for uses other than to permit Canadians to vote. The law now forbids any uses of the register other than for electoral purposes.

Updating by datamatching A second important reservation was the proposal to update the list by collecting voters' personal data electronically from other federal data bases such as income tax returns. This type of data match is invisible and violates a fundamental principle of privacy protection—informed consent.

The Commissioner recommended, and Elections Canada agreed, to match data only with the voter's active consent. A box will appear on next year's income tax return offering voters the option of having Revenue Canada transfer only current names, addresses and dates of birth to Elections Canada. Revenue Canada will **not** disclose any other details. New citizens can also ask Citizenship & Immigration Canada to send their information automatically to Elections Canada for inclusion in the voters register. Matches with provincial data bases, such as drivers' licences or provincial and municipal voters' lists, will have to comply with any provincial privacy laws.

Annual disclosure of lists to political parties Until this latest round of amendments, political parties and candidates received copies of the lists only when writs were issued for an election. These amendments allow for annual disclosures of lists to all parties running a candidate in a riding and to the current member, presumably because they will now be updated more or less constantly. The Commissioner considers annual disclosures excessive, not needed for the electoral process and potentially an inducement to more frequent canvassing. Nevertheless, Parliament approved annual disclosures.

No telephone numbers The Commissioner also recommended against collecting telephone numbers and including these on the lists provided to political parties and candidates, arguing that furnishing this information would make the electoral process the agent for telephone canvassing. Of course, political parties can buy software to blend the election lists with electronic telephone directories but they can do so at their own cost. Elections Canada dropped the telephone number from the data to be collected for federal elections (some provinces require the number for provincial elections).

Power to collect more data defined The provision allowing the Chief Electoral Officer to collect other personal data, once open-ended, is now more narrowly defined as that needed to "implement agreements with provincial bodies". The effect is to allow Elections Canada to collect additional details (such as

occupation) if they are required to vote in a province. Any additional information will not appear on lists compiled for federal elections.

The right to opt out The right not to be in the register was certainly the most fundamental privacy question and one which met no opposition from Elections Canada. Not being in the register will not deprive anyone of their right to vote but it will mean taking an active step to put one's name on the voters list, once an election is called.

Unfortunately, despite the best intentions, this aspect of the new process may have broken down. Based on admittedly anecdotal evidence from staff and callers at this and other commissioners' offices, enumerators seemed not to have understood the optional nature of the register. In fact, some told Canadians that if they were not in the register, they could not vote. However, enumerators cannot be faulted for misleading voters; they may not have been told. Privacy staff confirmed that the training materials did not mention the option; apparently the matter was to be dealt with verbally during the two-hour training sessions. Admittedly, training 96,000 enumerators across the country is a communications challenge, and teething troubles are hardly unexpected in an undertaking of this magnitude. Given the interest and the commitment of the Chief Electoral Officer and his staff to reinforce privacy in the electronic register, we hope and expect that the glitches will be remedied.

Anyone who was not properly informed and does not wish to be in the register can remove his/her name by writing to the Chief Electoral Officer at 257 Slater Street, Ottawa, K1A 0M6.

The Firearms Registry

The privacy issues surrounding the proposed legislation on gun control were evident in 1994 when it became clear that the government was contemplating a registry. Privacy staff met registry officials to discuss what information would be collected, by whom, where held, under whose control—and thus subject to what privacy law, if any. Managing the information was important because the model being contemplated bore some resemblance to the Canadian Police Information Centre (CPIC) which is a national police cooperative, administered by the RCMP, but not a federal undertaking and therefore only partly subject to federal privacy law. Its status had raised thorny jurisdictional issues for more than one privacy commissioner. (CPIC now has a national privacy policy to which all members must adhere.)

The *Firearms Act* (Bill C-68) passed Parliament in June 1995 with no specific privacy language in place and, given its hybrid nature, without the registry being made subject to the federal *Privacy Act*. The Commissioner was assured that privacy obligations would be spelled out in the regulations to follow and was encouraged to give his input then. The Senate Committee on Legal and Constitutional Affairs did not wait. Recognizing the privacy issues at stake, they called the Commissioner to appear.

In short, the Commissioner observed that the bill anticipated collection of substantial and potentially sensitive personal information which needed protection in the law or, failing that, in the regulations. Firearms registrars will maintain records of every licence and certificate issued and revoked, application refused, every loss, finding, theft or destruction of a firearm, as well as both exports and imports. In addition, local firearms officers, who may be provincial or municipal officials, will gather highly personal medical and domestic details on firearms applications. The Commissioner commended the *Privacy Act*'s fair information code as a model for appropriate collection, use and disclosure of any personal data needed for the register and recommended making those principles clear in the law.

In April 1996, regulations were submitted, then withdrawn and a new set submitted in November 1996. They provided very little detail. Nevertheless, the accompanying regulatory impact analysis stated firmly that "matters of access to the information kept, and the privacy of that information will be found in the relevant provincial and federal law" and that the "law is comprehensive and deals adequately with all the issues...".

The Commissioner begged to disagree. In a February 1997 appearance before the House of Commons Subcommittee examining the regulations, he pointed out first, that not all jurisdictions have privacy law. Second, some provincial privacy laws deal only with access to personal records and establish no rules on appropriate collection, use and disclosure of personal information. Third, some provincial laws do not cover the municipal police forces who often will gather and control the records. In short, there are gaping holes in the legal protection.

Since the regulations themselves provide little detail, it now appears that only the forms and schematic of the process will provide the answers—far too late to provide legal protection. Nevertheless, two regulations warrant particular mention. The first concerns procedures to obtain a licence which include the police notifying current and former spouses, and broad powers and discretion to gather "additional" information about applicants.

While the intent of the provisions are clearly to protect public and individual safety, the process needs some accountability to ensure the information is credible and relevant. Anyone providing information which is used to determine the applicant's suitability for a licence should be prepared to have their comments given to the applicant. Being able to face one's accusers is a fundamental principle of both privacy law and natural justice. Any deviations should be exceptional, not the rule. Having a comprehensive privacy scheme in place would enhance the accuracy and currency of the information by allowing applicants to correct factual errors and annotate disputed information. And some attempt should be made to define what types of "additional" information may be relevant to granting a licence so as to prevent "fishing expeditions".

The second omission is an interim review process for those denied a licence. The current scheme requires the unsuccessful applicant to go directly to court. Apart from the burden this places on both the applicant and, one would argue, the courts, it also risks disclosures of potentially sensitive personal details in an open process, some or all of which may be disputed. It seems a heavy-handed approach to challenging an administrative decision where an independent third party or panel would serve as well at lower cost.

The Subcommittee passed the regulations but made two recommendations to deal with the privacy issues. The first recommended that the government negotiate a memorandum of understanding with each province and territory, establishing that the *Firearms Act* is a federal statute, subject to the *Privacy Act* where no comparable provincial privacy law exists, and setting out rules of application in those jurisdictions. The government accepted the recommendation.

However, the government rejected the second recommendation for a mediation mechanism to allow applicants "to challenge allegedly false or inaccurate information without resort to court action". It argued that investigative techniques already ensure that the decisions are not based on inaccurate information and the investigations will normally give an applicant an opportunity to be heard. While it undertook to see whether the investigative process could be improved to deal with privacy concerns, the Department of Justice rejected mediation as "incompatible with the overriding safety objectives of the legislation".

The Commissioner is unconvinced.

DNA Databanking

On April 10, 1997, the government introduced Bill C-94, the *DNA Identification Act*, in Parliament. The purpose of the bill was to establish a DNA databank of samples taken from convicted offenders to help police identify those responsible for other unsolved crimes. The bill was the second phase of the government's scheme to regulate DNA testing as a tool to identify individuals responsible for certain crimes. Although it died on the order paper with the election call, several aspects of the Bill give cause for concern. There is now an opportunity to get it right.

But first, to backtrack. The first phase of the government's DNA testing plan was passed in 1995, allowing police to take samples without consent from individuals suspected of criminal offenses, generally those involving serious violence. The sample taken from the suspect would be matched with samples from the crime scene to determine whether the suspect had committed the specific offence being investigated. The legislation did not deal with the storage of the information—or samples—derived from the testing. This was one of a number of issues left for the second phase.

We cautiously supported the 1995 legislation. DNA evidence can help convict the guilty and absolve the innocent, and the 1995 legislation provided a reasonable scheme to ensure that DNA samples were not taken from suspects unnecessarily. Then, early in 1996, the Solicitor General issued a discussion paper (*Establishing a National DNA Databank*) which examined several other issues, including the storage questions, and asked for comment.

Our response to the discussion paper made several suggestions for the government to consider before introducing legislation. Among them were three major conditions that needed to be met to satisfy privacy concerns:

- reviewing the legislation within three to five years of its enactment, including a privacy audit to determine to what extent the intrusion involved in creating a database was justified by an increased number of violent crimes solved through DNA evidence;
- taking DNA samples only from those convicted of a violent offence for which there is a high risk of re-offending and a high likelihood that genetic material would be left at the crime scene, and
- destroying the DNA samples after extracting the identification information, leaving only the analysis on police files.

Bill C-94 did propose a general review of the legislation within five years of its enactment. However, its treatment of the other issues is problematic.

The "designated offenses" First, the range of offenses for which samples could be taken from convicted offenders appears unnecessarily broad. It may seem trivial to quibble over the criminal offenses for which the state could compel offenders to provide a DNA sample. It is not. This technology empowers the state to intrude into our very bodies—a power it should exercise only in the most compelling circumstances. Casting the net too wide results in privacy intrusions on a massive scale.

The Bill contained a list of "primary designated offenses"; generally serious, and frequently violent, crimes such as manslaughter, sexual assault and kidnapping. Taking a DNA sample is automatic on conviction for these offenses. However, a list of "secondary designated offenses" for which police may seek a warrant for a DNA sample includes (among others) common assault, breaking and entering, setting fire to "other substances" and failing to stop at the scene of an accident.

Storing the DNA samples Among our most serious reservations about Bill C-94 is the plan to store the DNA *samples* themselves, rather than just the *analysis*—the information drawn from the samples. This is not too fine a distinction to make. This legislation seeks to use DNA to link specific offenders with specific crimes. Keeping the DNA sample itself will inevitably invite further uses of the DNA that have little to do with identifying offenders; for example, allowing researchers to use the material to study genetic links to criminal behaviour. This century has already seen one misapplication of genetic research to criminal behaviour (the XYY chromosome theory which purported to identify violent males).

We remain strongly opposed to retaining DNA samples. Analysis of the DNA is sufficient to help police solve crimes, without the need to preserve the actual sample.

The policy makers behind Bill C-94 had a choice. They could choose the least intrusive measure; retaining the information they needed for forensic DNA identification, or the most intrusive measure; keeping the DNA samples themselves. They chose the latter.

The seriousness of the privacy invasion—allowing the state access to our bodies—warrants the least intrusive means. That means storing identifying information only. Should keeping only the analysis prove an unworkable limitation on investigations, the subsequent review would allow Parliament to address the issue. By adopting the most intrusive measure first, we will have no

way of knowing whether the lesser intrusion would have been sufficient. And few of us would expect the state to surrender a power once it is acquired.

We also continue to be concerned about authorizing police officers to take DNA samples. There is something chilling about a police officer, not medical personnel, performing what is essentially a forced medical procedure, no matter how minor or painless.

Destroying "volunteered" samples The bill is silent on another source of concern—the treatment of DNA samples from "volunteers". A recent sexual assault case in Vermilion, Alberta illustrates the problem. Police asked male residents to volunteer DNA samples to help eliminate them as suspects in an investigation (in other words, to prove their innocence, an odd twist to one of the fundamental presumptions of our criminal justice system).

Having given the police a DNA sample for that investigation, the volunteer should have a right to have that sample and any analysis destroyed immediately after it has proven that they were not implicated. DNA samples taken from volunteers should never be retained, and the analysis of those samples should never be kept for a database. Nor should they be used to investigate any crimes other than the one for which they were gathered, unless the person gives a fully-informed consent to further uses.

Unfortunately, Bill C-94 offered no provision to ensure that volunteered samples and any information relating to them would be destroyed as soon as they proved the donor's innocence.

Reopening the DNA issue on another front

On April 14, 1997, shortly after Bill C-94 was introduced, the Canadian Police Association (CPA) placed full-page advertisements in *The Hill Times* calling for extending the current law on identification of criminals to DNA technology:

[T]he current law, pursuant to the *Identification of Criminals Act*, which permits the taking of offender information (fingerprints) at time of arrest for indictable offenses, [is] exactly the process which must be followed with the technological upgrade which DNA samples represent.

The Association appears to advocate taking DNA samples, like fingerprints, *as a matter of course* from anyone arrested for an indictable offence. It is clear that the Association wants to use the DNA databank bill to obtain expanded powers to take DNA samples from *suspects*—the issue that was the focus of the DNA legislation passed by Parliament in June 1995.

CPA's attempt to expand the taking of DNA samples from suspects is extremely troubling. DNA samples cannot be equated with fingerprints. True, both offer information that can identify an individual. Fingerprints do no more. However, human DNA contains a storehouse of highly personal information that has nothing to do with linking a person with a crime, and that can be seriously damaging to an individual if allowed to fall into the wrong hands.

The office has spent considerable energy ensuring that DNA samples could be collected from suspects where warranted, while respecting the legitimate privacy rights of Canadians. Apparently the points we made in our first (1995) submission on the issue of forensic DNA analysis bear repeating:

DNA evidence should **not** be collected from suspects as a matter of routine. To do so causes an unnecessary privacy intrusion; in the vast majority of criminal cases DNA evidence will contribute nothing to the investigation. Thus, it would not be appropriate for Parliament to give blanket authority to collect DNA samples from all persons suspected of indictable offenses. DNA should also not be collected from a suspect if investigators have no DNA evidence with which to compare the suspect's sample.

Nor would a DNA sample from the suspect be necessary if the suspect admitted guilt. However, as a practical matter, the DNA evidence might be critically important in getting the suspect to admit guilt in the first place.

...

In short, we recommend the following conditions on the collection of DNA samples from suspects:

- (a) the crime must involve violence or the likelihood of violence
- (b) there must be reasonable grounds for suspecting that the person committed the offence
- (c) a DNA sample must be relevant to proving the offence; investigators must have DNA related to the crime with which the suspect's sample can be compared, and
- (d) the collection from the suspect must be authorized by a judge.

Our position was largely reflected in the DNA legislation passed in 1995. Now, however, the CPA wants to remove three of these four privacy safeguards: the requirement of a *violent* crime, the relevance of the DNA sample to proving the offence, and the requirement of a judicial warrant.

The CPA's proposal would also lift the restriction, accepted in the 1995 law, that a sample taken under warrant be used only to investigate the offence in question.

The thirst for ever greater police "efficiency" by using intrusive technologies—technologies that may not live up to their promise—must not be allowed to override this fundamental right of privacy without a clear and compelling justification. The CPA has offered no such justification.

Position papers on both issues, compulsory collection of DNA samples from suspects in a specific crime and establishment of a DNA database, are available from our office and at our Internet web site; <http://infoweb.magi.com/~privcan/>.

Where Should Parliament Draw the Line?

In April 1997, shortly before Parliament was dissolved for the federal election, the House of Commons Standing Committee on Human Rights and the Status of Persons with Disabilities issued its report, *Privacy: Where do we Draw the Line?* The committee, chaired by the Hon. Sheila Finestone, examined a range of privacy issues flowing from new technologies. The report is a must-read for anyone interested in preserving some vestige of their privacy.

Mrs. Finestone referred to the stunning impact of reports from the Privacy Commissioner of Canada and subsequently from specialists, on the wide-ranging capabilities of new technologies and their implications upon the right to privacy.

To the committee's great credit, it did not merely listen politely to those concerns, then walk away—as some Parliamentary committees have done. Instead, the human rights committee concluded that it was time to "explore the role of privacy as a human right and social value". The committee soon realized the importance of its mission: "As we struggled with the impact of new technologies on our understanding of privacy, we realized that, ultimately, we were talking about what kind of society we want for our future".

To make its task even remotely manageable, the committee focused its examination on the privacy impact of three technologies on peoples' lives—advanced video surveillance, genetic testing and smart cards. These, the committee report argued, were examples of technologies on the cutting-edge where real choices will soon have to be made.

The committee's work had two phases. First, members heard from a range of international privacy experts (many of them, we are proud to say, Canadian). Second, it conducted a series of "town hall" meetings across Canada to learn how Canadians felt about their privacy and the government's role in protecting that right.

The committee's task was truly daunting. Our office is often overwhelmed by the growing number of instances where technologies threaten the fundamental human right of privacy. For a Parliamentary committee, whose members all had multiple other responsibilities, addressing even a handful of these important issues would not be easy.

Despite the magnitude of its task, what emerged from the committee's ten months of consultations and research was an intelligent and thoughtful program

for government to begin addressing the privacy threats Canadians face at the end of this century.

Most important, the committee reinforced the importance of privacy as a fundamental human right. The committee's proposed Canadian Charter of Privacy Rights, a kind of "quasi-constitutional" document that would take precedence over other federal legislation, would guarantee the expectation and enjoyment of

- physical, bodily and psychological integrity and privacy;
- privacy of personal information;
- freedom from surveillance;
- privacy of personal communications, and
- privacy of personal space.

These rights could be infringed only if the interference were reasonable and could be demonstrably justified in a free and democratic society. In other words, privacy should be the natural state of affairs; a right of Canadians that should not require justification. Instead, the onus would rest with government (or the federally regulated private sector, such as banks, to which the Charter would also apply) to justify privacy intrusions.

The report also calls on the government to introduce legislation to "deal specifically with the privacy and antidiscrimination issues related to genetic testing", as well as amendments to the *Criminal Code* to extend current prohibitions against interception of private communications to surreptitious video surveillance.

Some of the committee's recommendations would have significant impact on the Office of the Privacy Commissioner.

The first calls for replacing the current *Privacy Act* with a *Data Protection Act* which would extend privacy protection to personal information held by Parliament, all federal government departments, agencies, Crown corporations, boards and commissions, and the federally-regulated private sector. (The current act applies only to approximately 105 federal bodies named in the schedule—government departments for the most part.) An important part of the new law would be stricter rules on data matching within the federal government and data sharing between the federal and provincial and territorial governments.

The committee also recommends new legislation to broaden and strengthen the mandate and powers of the Privacy Commissioner to deal with privacy issues in the federal sector. In addition to the Commissioner's current obligations to both receive and initiate privacy complaints, the committee recommended empowering the Commissioner to conduct audits, technology impact assessments and studies on privacy and emerging technologies. It also advocated that the Commissioner review legislation, regulations, policies and practices that may have an impact on privacy rights and, when appropriate, table a privacy impact statement before the House of Commons.

The legislation would be preceded by a broad and open public consultation process and also provide for a comprehensive public review of its provisions and operations within five years (and at regular intervals thereafter).

Among the committee's many other recommendations:

- an explicit constitutional right to privacy in the long term;
- framework data protection legislation governing the federally-regulated private sector;
- efforts to build generally uniform privacy laws across the country;
- access to and use of privacy enhancing technologies, and support for the creation and availability of such technologies;
- greater public education about privacy issues, and a formal education mandate for the Office of the Privacy Commissioner of Canada;

The committee's report is a voice of salvation for the too-often besieged right to privacy of Canadians. The report calls for much of what this Office has long advocated, and proposes much else that we can comfortably support. The challenge now is to translate the committee's concerns into action. A new government may have new priorities—we will do our utmost to ensure that acting on the committee's report becomes one of them.

Privatization and Devolution: Who's in, who's out?

The discussion in last year's annual report about the privacy implications of government privatization met with some puzzled responses. Why was privacy a concern? The case most immediately at issue was Transport Canada's transfer of the air traffic control system to NAV CANADA, a not-for-profit corporation.

However, NAV CANADA was simply the first of a number of federal agencies undergoing metamorphoses; some simply into new government agencies, some into private but not-for-profit organizations, and others into private companies. The common thread was that no provisions were being made to continue the privacy rights acquired by clients and employees of the organizations.

Early in 1995, the Privacy Commissioner alerted government and the public to the apparently unanticipated consequence of contracting out services and handing off federal operations to the private sector. In his report to the Standing Committee on Government Operations, the Commissioner recommended that the government

- issue a broad policy directive that all personal information handled by the private sector for, or in lieu of, government remain the property of the Crown and subject to its control for purposes of the *Privacy Act*;
- require all government institutions subject to the *Act* to insert comprehensive data protection provisions in contracts with the private sector;
- prohibit federal institutions from reducing the scope of privacy rights as a consequence of dealing with the private sector, and
- in the interim, extend the *Privacy Act* to cover all federal institutions and all federally-regulated private sector enterprises.

Soon after the creation of NAV CANADA, the government offered for outright sale the printing operation of the Canada Communication Group (CCG), formerly the Queen's Printer. The Privacy Commissioner wrote to the deputy heads of both Transport Canada and Public Works and Government Services (PWGS) asking that they commit to maintaining privacy protection. Neither deputy agreed.

In his mid-1996 appearance before the Commons Transport Committee, the Commissioner recommended making NAV CANADA subject to the *Privacy Act* to ensure continuing privacy protection. He also alerted members to the perils of privatizing a substantial government operation without the benefit of a cogent

information management plan. The Committee agreed and recommended the government include the provision in the enabling legislation. NAV CANADA resisted, the government ignored the recommendation and the legislation passed unchanged.

Staff also approached CCG to offer input on reviewing the personal records it anticipated transferring to St. Joseph Corporation, the new owners. CCG accepted and over the ensuing months it prepared its personal files for the sale. The transferred files now include only those concerning corporate clients, and employee files containing only essential information—name, business unit, position title, salary, preferred language and seniority. All affected employees signed an undertaking that they had no confidential government or personal information except their own. All personal information contained in filing cabinets and work stations was removed to a central repository under the control of PWGS where it will be properly maintained or destroyed. And all computer memories were erased before being released to St. Joseph Corporation.

Paying the piper When Bill-C20 cleared both houses of Parliament with no privacy protection clauses, the Commissioner initiated a review (under section 37) to satisfy himself that the transfer of personal data to NAV CANADA complied with the *Privacy Act*.

As anticipated, the audit team discovered that most personal records could not easily be transferred because they contained an abundance of personal data that did not fall within the scope of the transfer protocol. Nor had any attempt been made to seek the consent of the individuals concerned. At the 11th hour, Transport Canada was required to hire staff and review masses of personal documents. (See page 49 for detail).

While the Office's attention was focused on CCG and NAV CANADA, government announcements to privatize or devolve other government programs arrived at a steady pace—manpower training programs transferred to the provinces and to Indian Bands; airport and port authorities devolved to other levels of government or converted to Crown corporations; the St. Lawrence Seaway to join ranks with NAV CANADA as a private sector "not-for-profit" corporation. And—just passed or on the drafting tables—new agencies to inspect our food, collect our taxes, and monitor our health.

The Commissioner sought the help of the Clerk of the Privy Council and the Deputy Attorney General to stem the haemorrhage. He asked for a commitment that privacy rules would apply to all new privatization and devolution initiatives. He also asked to be informed of any new initiatives at the earliest possible date.

A March 17, 1997 letter, signed jointly by the Deputy Attorney General and the Secretary of the Treasury Board, advised the Commissioner that:

"... in principle, when programs or services of the federal government are privatized or commercialized, continuing protection of personal information equivalent to that contained in the *Privacy Act* should be made part of the agreement between the government institution and the private sector entity taking over the responsibility. We are working to develop a clear government policy statement to that effect.

In addition, as the government has already committed itself to the introduction of legislation in the federally-regulated private sector, it makes sense that any newly created federal government institution should be added to the schedule of the *Privacy Act*".

As we go to press, we have not yet seen a clear government policy on the subject, but we can report that Human Resources Development Canada has made considerable efforts to ensure privacy protection is addressed in its negotiations to devolve responsibility for manpower training. The Canada/Alberta Service Centres agreement serves as an example.

Bill C-60 creating the new Canadian Food Inspection Agency recently passed into law. It binds the new agency to the *Privacy Act*. Bill C-44, the *Canadian Marine Act*, died on the order paper, however, it also contained a provision to make all of Canada's major ports subject to the *Privacy Act*. And the first draft of plans to create the new tax collection agency include a provision making the agency subject to the *Privacy Act*.

It is difficult to understand why ports and a crown corporation like Canada Post are subject to the *Privacy Act*, but not airports, or not-for-profit monopolies like NAV CANADA and the St. Lawrence Seaway Authority. Perhaps it's just timing—little consideration was given to privacy protection in the early rush to privatize—or perhaps the NAV CANADA audit illustrated our point. Whatever the reason, the federal government now has in place a more systematic approach to privacy protection and privatization.

Publicizing the Identity of High-Risk Offenders—an update

Last year's annual report discussed at some length the challenges of finding a balance between society's need to protect itself from violent criminals, and the need of individuals who have served their sentences to re-enter society. While publicizing some offenders' identity may help the community adapt to the person's presence, publicity could increase the risk of harm to, rather than protecting, the community.

Since last report, there have been three developments of note.

First, Parliament amended the *Criminal Code*, the *Corrections and Conditional Release Act* and other federal statutes concerning offenders who pose a high risk of committing further violent offenses. A court may now designate a person convicted of certain sex offenses as a long-term offender, providing certain conditions are met. The court must then order the offender to be supervised in the community for up to ten years.

Identifying individuals as long-term offenders gives police and correctional authorities the right—and duty—to supervise them in the community after their release from custody. Effective supervision by police and correctional authorities may reduce the need to notify the community about the presence of an offender in their midst.

The same set of amendments introduced a new provision to the *Criminal Code* allowing Crown prosecutors to ask a court to require a person to enter into a recognizance to keep the peace, "be of good behaviour", and comply with any other conditions the judge sets out. Prosecutors can use this provision in cases where they have reasonable grounds to fear that the person will commit a serious personal injury offence. This provision allows some control over violent offenders who are released into the community at the end of their sentences.

Since last year, several provinces have developed protocols, either by law or policy statements, establishing when it is appropriate to notify communities about the presence of certain released offenders.

In November 1996, Saskatchewan proclaimed in force *The Public Disclosures Act*. The Act sets in place a means for a police service to ask a "public disclosure committee" appointed under the Act to decide whether information about an

individual should be released to the public, and the extent of the release. The police force would make the final decision whether to release the information.

In April 1997, Alberta introduced a protocol on the release of information that would apply to any convicted person judged to pose a risk to others. Newfoundland (1996) and Yukon (1997) also introduced protocols. Ontario's *Community Safety Act*, also a vehicle for the release of information about high risk offenders, was introduced in the Legislature in 1996, but has not yet been enacted.

Also in April 1997, the Nova Scotia Department of Justice released for discussion a draft protocol on disclosure of information about high risk offenders. The Nova Scotia protocol proposes to establish a community notification advisory committee to which police forces could refer cases. However, the police agencies themselves, not the committee, would make the final decision about any release of information.

The difficulty of finding the right balance in the debate over notification is illustrated in a recent Ottawa case. A convicted paedophile was released at the end of his sentence. Media reports suggested that he was at considerable risk of re-offending. His identity was discovered by the community and a newspaper published his photograph on the front page. Shortly afterwards, the offender moved. His new location was unknown. In fact, he had simply moved from the centre of town to a suburb where, despite the media publicity, his criminal history remained unknown for months.

This underlines one of the flaws in publicizing offenders' identity in the community. Despite the extensive coverage of his photograph, the offender was able to reestablish himself—for several months, at least—in another community in the same metropolitan area. Publicity in this case appeared to do little good and may have driven the person underground.

The same case illustrates yet another potential harm from publicity. Eventually, the offender's identity was discovered, and he was severely beaten by a local resident—a vigilante action that will succeed only in driving the offender to yet another community, where he will have an even greater incentive to keep his past secret.

Just before this report went to press, the Commissioner spoke at a national conference on community notification in Winnipeg. Conference participants discussed the competing interests and examined several notification schemes, as well as other legal mechanisms for protecting public safety. We will continue to follow the issue closely.

This Year's Telecommunications News

Directory listings: The saga continues

Last year, we reported on efforts by independent telephone directory publishers to buy the electronic subscriber lists of full-service telephone companies. The Canadian Radio-television and Telecommunications Commission (CRTC) agreed but asked the telephone companies to give their subscribers an opportunity to remove their names from the lists before sale to independent publishers.

White Directories, one such publisher, argued that allowing telephone subscribers to opt out of the sale would mean independent directories would be less complete than those of affiliated publishers (such as Tele-Direct, Bell Canada's directory publisher). White appealed to the Cabinet that it would be at a competitive disadvantage. In June 1996, the Cabinet agreed, overturned the CRTC decision and asked it to report on two issues: the appropriate level of protection to be given to subscriber listings, and the mechanisms for unlisting one's name and number from any directory. The CRTC called for submissions from interested parties.

In his September 1996 submission, the Privacy Commissioner observed that most telephone subscribers understand that their listings will be used for directory assistance and to publish the local telephone directory. However, they are not told that the lists are rented and sold to competing publishers and marketers, or that their listing is available through call-display and call back options. Those wanting an unlisted number are further discouraged by the cost which ranges from \$1.55 to \$5.75 a month.

The Commissioner recommended that:

- the telephone companies spell out all the listing options for subscribers;
- not charge for unlisted service, and
- provide unlisted subscribers with free per-line blocking and ensure the blocked listings are only available for emergency and lawful call tracing purposes.

He also urged the CRTC to prohibit other directory publishers from contacting unlisted subscribers (using other information sources) to promote listing in their directories, and to require them to establish a means for individuals to de-list should they choose to at a later date.

Of course, suppliers of all telecommunications services assemble lists of their clients; companies selling cellular telephones, pagers, PCS, and Internet services all assemble customer lists and commercial Web sites maintain lists of site visitors. Some of these companies publish or sell their lists. For example, America On-Line recently sold its subscriber lists to a list broker—a company which specializes in the sale of mailing lists targeted for commercial interests.

Providers of these services should be required to spell out the primary and secondary uses of subscriber listings and seek consent for such secondary uses as sale to third parties.

In its December 1996 report, the CRTC agreed subscribers needed to be better informed of their listing options, observed that the privacy of fax and cellular subscribers was well protected by existing listing mechanisms, and acknowledged that existing costs deterred subscribers from choosing to be unlisted. The CRTC will hold public hearings on unlisted charges and the Privacy Commissioner will participate.

Going digital: No miracle privacy solution

Many readers remember media stories about intercepting conversations on cellular telephones. Most existing cellular phones transmit in analog format (conventional radio waves) and are easily intercepted using cheap off-the-shelf scanners.

One way to avoid interception of cellular calls is encrypting the signals to make them incomprehensible to the interceptor. However, encrypted analog signals are easily unscrambled. Another method of protecting one's calls is to transmit signals in digital format (the 0-1 binary code used by computers). Digital signals cannot be intercepted by analog scanners. But neither is "being digital" the ultimate solution.

Digital signals can be intercepted: Digital scanners, now rare and expensive, will gradually become more widely available and cheaper. In October 1996, Industry Canada acted on an earlier undertaking and issued Standard RSS-135-1 obliging digital scanner users to obtain a license. However, the licensing requirement will not apply to users of manually-tunable digital scanners, the bulk of the digital scanner market.

Encrypted digital signals can be unscrambled: Although digital encryption is far better than analog encryption, it can still be decoded, as proven in March

1997 by researchers from the University of California at Berkeley and a private U.S. systems company.

Digital signals do not always remain digital: Digital signals are automatically converted back to analog format if any point on the transmission path cannot support digital signals; for example, when the receiver is using an analog cellular phone or a conventional analog home telephone. The moment the signals become analog, they can be intercepted more easily. (Of course, once the conversation is carried on conventional wires, it is protected by the wiretapping provisions of the *Criminal Code*

These cautions apply equally to all digital wireless services such as Business Communications Systems (BCS), Enhanced Specialized Mobile Radio, Local Multi-point Communications Systems (CellularVision Canada, MaxLink Communications and Regional Vision Canada), pagers, Personal Communications Systems (PCS), and wireless telephones.

In the Courts

Privacy Commissioner of Canada v. Canada Labour Relations Board et al— Court File A-865-96

In this case, the Privacy Commissioner supports an individual seeking access under the Privacy Act to his personal information recorded in hearing notes by two members of the Canada Labour Relations Board. The Trial court judge rejected the application in June 1996 and the Privacy Commissioner has appealed that decision to the Federal Court of Appeal. At issue is the definition of personal information, the notion of agency control of that information and the nature of the exemptions under the Act. Also at issue is the extent to which Board members may claim judicial independence in the same manner as judges of the courts.

Intervenors are the Public Service Staff Relations Board, the Human Rights Tribunal, the Canadian International Trade Tribunal, the National Transportation Agency of Canada and the Attorney General of Canada. The appeal is expected to be heard in the Fall.

Michael A. Dagg v. the Minister of Finance and Privacy Commissioner of Canada and Public Service Alliance of Canada—Court file S.C.C. 24786

In this case, Mr. Dagg requested access under the *Access to Information Act* to logs signed by employees entering and leaving the Department of Finance, after hours. The Minister provided access to the logs but deleted employees' names, identification numbers and signatures, considering this information personal. Mr. Dagg complained to the Information Commissioner who supported the Minister's decision to withhold the information.

Mr. Dagg applied for a review of the Minister's decision and succeeded at Trial. He lost subsequently at the Federal Court of Appeal and has now succeeded in this first case to come before the Supreme Court of Canada dealing with personal information under the *Privacy Act*. In a split 5/4 decision, the Court held that the information Mr. Dagg sought relates to the individual's position and not to the individual. Therefore it falls within an exception to the definition of personal information in the *Privacy Act* and thus may be accessible under the *Access to Information Act*.

However, the decision is fundamental for the guidance it provides for reconciling two apparently competing legislative policies—access to information held by the federal government, and protecting the privacy of individuals' personal information in those records. The Court stated that both statutes recognize that, once information meets the definition of "personal" in s. 3 of the *Privacy Act*,

privacy is paramount over access. Further, the Court held that the general opening words of the definition—"...information about an identifiable individual..."—are intended to be the primary source of interpretation for what constitutes personal information. Justice La Forest continues, "Consequently, if a government record is captured by those opening words, it does not matter that it does not fall within any of the specific examples"

Finally, the Court endorsed a deliberately broad definition as consistent with the great pains which Parliament has taken to safeguard individual liberty. "Its intent seems to be to capture **any** information about a specific person, subject only to specific exceptions...". The Court continues, "Such an interpretation accords with the plain language of the statute, its legislative history and the privileged, foundational position of privacy interests in our social and legal culture."

Incidents

Tax audit documents found in surplus file cabinet

A broadcast journalist alerted the office to several taxpayers files found in an old filing cabinet. The journalist made two copies of the documents, gave one set to the radio station's legal counsel and sent the second to the Commissioner. The originals were returned to the finder who subsequently turned them over to his MP.

Once the Commissioner examined the papers, it was evident that they were tax audit files which also contained banking and real estate documents about nine taxpayers. The investigator returned the files to Revenue Canada and began an inquiry.

The cabinet appeared to be one of more than 275 sent by Toronto North Tax Services to a Crown Assets Distribution Centre between March and June 1996 for resale. The cabinets were declared surplus following a major refit of offices to maximize space and accommodate GST staff being moved from another building. Employees affected by the move were temporarily shifted to other floors and the surplus cabinets assembled for eventual sale. The buyer purchased the cabinet at the Mississauga disposal centre and, on opening it, found documents in the first drawer. He then found more documents behind a divider in another drawer. Disturbed by the carelessness, he called the journalist.

Although the investigator could not establish conclusively that the cabinet was from Toronto North, it is highly likely. During that move, employees were reminded to check their cabinets thoroughly and other staff conducted a spot check but did not search every one. Although clearly a human error, Revenue Canada has reviewed its operating practices and taken extra steps to prevent a recurrence.

The Commissioner asked Revenue Canada to notify the taxpayers whose files were disclosed, apologize and explain the circumstances. He also pointed out that the files themselves contained old working papers which do not form part of the official audit file. Revenue Canada appeared not to have a retention and disposal schedule for these documents and some were kept indefinitely. The Commissioner recommended Revenue Canada consult National Archives on an appropriate schedule and describe the material in *Info Source*, the government directory of information holdings.

Canada Post copies courier competitors' client addresses

Another journalist alerted the office to a sales blitz going on at the Longueil postal station near Montreal. Apparently keen sales staff were encouraging postal sorters and carriers to photocopy the envelopes, or note the addresses, of mail from nine competing courier companies. With the clients' addresses, the sales staff planned to approach the competitors' clients and try to sell them Canada Post services.

To encourage staff to participate, \$1 per prospective client would be paid into the appropriate unit's social fund and, ultimately, names of participating staff would be entered in a \$50 draw.

The portfolio officer called Canada Post which immediately acknowledged that the promotion was wrong and senior management was taking it very seriously. The specific question of whether it was also a violation of the *Privacy Act* hung on whether the addresses were individuals' homes, rather than business addresses and titles.

While staff pursued this avenue, the Minister was questioned on the incident in the House of Commons. She replied that the promotion was an error, an isolated incident, it would stop and it would not happen again. The Canada Post president obtained written assurances from all vice presidents that this was not general practice. The manager and three sales staff were disciplined. And, finally, all sales staff will be required to take an ethics course and sign a written statement acknowledging that they have taken and understood the course.

Given Canada Post's vigorous and speedy action, the Commissioner considered the incident resolved. Any individual complaints would be investigated in the usual way.

Stamp collector's credit card billed for unordered products

Another Canada Post business practice offended a stamp collector who found himself billed for stamps he had not ordered. Although an occasional purchaser of Canada Post products, paid for by credit card, he had not ordered the "Winnie the Pooh" series. The stamps arrived, billed to his credit card, with an explanation that if he did not want them, they could be returned for a credit.

A journalist called to ask whether this was a violation of the *Privacy Act*—misuse of the credit card number which had been provided for specific purchases. Although the office did not receive a direct complaint, Canada Post did—150 of them.

Privacy staff undertook to resolve the matter informally. The first hurdle was for Canada Post Marketing staff to recognize that misuse of a credit card number was a privacy issue. Although they acknowledged the marketing mistake, they needed convincing that taking information provided for one purpose, then using it for another without the client's consent, is a violation of the collection principles in the *Privacy Act*. Canada Post's privacy coordinator undertook to explain the principles to marketing staff.

The second hurdle for Canada Post was to sort out the permutations and combinations in client lists. Many stamp collectors have a standing order for all new stamps to be billed automatically to their credit cards. Some collectors have standing orders but for specific interests—first day covers, special issues, those displaying the crown—and may, or may not, want to be alerted to other products. Others want to decide on each issue. The standing order lists were not always clear. They needed cleaning up, and the options clarified.

As a result of the incident, Canada Post Marketing is surveying all standing order customers, explaining the product ranges, and asking them to identify the range to which they want to subscribe. This should help prevent customers being shipped and billed for products they do not want.

Health Files in Winnipeg trash bins

A journalist's call about a discovery of immigration medical files and X-rays in a Winnipeg trash bin sent an investigator on site.

According to the article, the originals of at least 300 preliminary medical examinations for individuals seeking entry into Canada were found overflowing trash bins in a Winnipeg alley. The documents, dating back to the 1970s and early 1980s, were found intact in Health and Welfare Canada envelopes and included applicants' photos, X-rays and personal medical information.

The medical documents had been placed in two bins behind a townhouse. The plastic bags had ripped, spilling some of the contents onto the ground. A resident collected the loose material, put it back in the bin and called Immigration Canada officials at the Winnipeg Airport, hoping they would retrieve it. Not satisfied with their response, she telephoned the *Winnipeg Free Press* and, finally, the police.

The investigator interviewed several parties and pieced together the story. A Citizenship officer received a call from an Immigration Officer at the Winnipeg Airport who reported being called about a large amount of immigration medical documents in garbage bins. The Citizenship officer went to investigate.

He discovered two garbage bins filled with many X-ray envelopes and other medical documents, some with photos attached. All appeared to concern persons seeking immigration to Canada. Some of the documents bore Health and Welfare identification. Unable to find a Health & Welfare contact, he called the Winnipeg manager of Citizenship and Immigration Canada, advised him of the discovery and later called to advise him that the bins would be emptied the following morning.

The following morning, two Health Canada employees learned of the discovery from the newspaper article. Their search for the records lead them through garbage bins over a three block area at the site, an attempt to locate the truck which had already emptied one bin, and ultimately to the Brady Road landfill site. They and two other employees searched the area where the truck had dumped but found nothing. Finally, city tractors buried and compacted the area so that any records were unlikely to be accessible to anyone.

Apparently the medical records had been stored at National Archives records centre in Winnipeg. The material was due for disposal and after a cursory inspection indicated that they contained only X-ray films, they were sold through Crown Assets to a local contractor for silver extraction. However, instead of providing just the X-rays, Archives turned over envelopes containing individual medical files of more than 2,600 potential immigrants to Canada.

The contractor who purchased the materials for silver extraction got a lot more work than he bargained for. He had sorted through approximately 300 paper files to extract the X-rays and put the paper in the garbage bins when journalists from the *Winnipeg Free Press* arrived to take photographs. He realized the material should not have been put there and went back immediately to retrieve the files.

While the newspaper stories and calls from various government officials unnerved the man, he returned all the documents and X-rays to Archives.

Health Canada had approved the disposal of the outdated records, as had Archives which agreed that X-rays of prospective immigrants have no historical value. Understanding the records contained only the X-rays, the Records Centre manager sent what was described as “1200 lbs of X-rays—silver content recoverable” to Crown Assets where the contractor’s bid was accepted.

An Archives staff member told the investigator that he examined more than ten envelopes and they contained only X-ray films, not medical reports. He removed any identifying details, marked the material to be disposed of as unclassified waste and it was moved to the shredding area. Other staff saw the

material with medical documents and photographs stapled to the outside of envelopes standing in the area and assumed they were to be shredded. The supervisor of the shredding company who was on site also confirmed that the skids had been placed in the shredding area and he was told that someone would pick the material up. He also confirmed that when the contractor arrived, he opened one or two envelopes and was surprised to see medical records in the envelopes, saying he thought that he had bought X-ray films.

The contractor also confirmed that all but two of about 300 X-ray envelopes he processed contained medical reports, the majority stapled to the outside. When the material was returned to the Records Centre it was found to consist of hundreds of loose X-ray films, envelopes and medical reports, as well as more than 60 bundles containing an average of 40 to 45 X-ray envelopes each. The centre compared the material against the accession shelf lists to verify that all the records have been returned.

The investigator confirmed that, in addition to X-ray films, they contain sensitive medical information about prospective immigrants to Canada, including applicants' photos, preliminary medical examination report, radiological reports and laboratory test results indicating whether the applicant had such conditions as a sexually transmitted or contagious disease. The review also confirmed that personal information, such as the individual's name, passport number, month/year of birth or age, address, etc., was also contained on the X-ray films.

The Commissioner found the officials of the Manitoba Region Federal Records Centre negligent in their handling of the records and sale of the X-rays. The disclosure of this material to the contractor was a direct violation of the disclosure provisions of the *Privacy Act*. The Commissioner made several recommendations to the Chief Archivist including

- suspending all sales of X-rays until new procedures are in place;
- removing film from the envelopes and destroying any identifying material;
- requiring contractors and staff having access to X-rays to sign undertakings of confidentiality;
- improving record centre staff awareness of what constitutes "personal information" and their obligations to protect it, and
- notifying the Commissioner's office without delay in similar cases in future.

The Archivist accepted all the Commissioner's recommendations and also suspended further sales of X-rays until the cost of silver recovery made the

operation cost-effective. In the meantime, the film will be destroyed in RCMP-approved equipment.

Audits

The Office has substantially reduced its dependence on audits as a method of assessing compliance with the *Privacy Act*. Systematic auditing has proved unsustainable with the Office's dwindling resources. Staff undertook two routine audits this year; the Canada Student Loan Program of Human Resources Development Canada and the RCMP Public Complaints Commission. A third, the Air Navigation System files of Transport Canada, were audited prior to their transfer to NAV CANADA.

Transport Canada - Nav Canada

Transferring the Air Navigation System (ANS) is one of the federal government's largest commercialization projects. The ANS includes seven Area Control Centres, 44 control towers, 88 Flight Service Stations and a network of navigation aids. It manages all Canadian airspace and designated International Civil Aviation Organization airspace in the North Atlantic Region, providing air traffic control for approximately 6.8 million aircraft movements annually. Under the agreement, NAV CANADA bought all relevant physical assets and assumed responsibility for approximately 6,400 employees.

In mid-1996 the Privacy Commissioner appeared before the Commons Transport Committee and urged that NAV CANADA be made subject to the *Privacy Act* to ensure continuing privacy protection for clients and employees. The Committee agreed and recommended the government include the provision in the enabling legislation. NAV CANADA resisted, the government ignored the recommendation and the legislation passed unchanged.

Given the size of the system and the potential disclosure of vast quantities of personal information, the Commissioner launched an audit of the transfer to NAV CANADA. In August 1996, staff began examining files in the National Capital and Quebec Regional Offices, Ottawa and Dorval air traffic control towers and the Training Institute in Cornwall. They identified several problems, including substantial amounts of personal information that was outdated, information that NAV CANADA did not need and, in some cases, sensitive information from managers' working files that should not have been collected at all.

However, the most immediate problem was the November 1, 1996 deadline for handing over the system to NAV CANADA—not enough time to complete what clearly was a necessary review. The Privacy Commissioner wrote to Transport Canada's deputy minister setting out the preliminary findings. Transport Canada agreed to extend by 60 days the proposed transfer date for personnel files and hired 35 temporary clerks to review files and cull extraneous information.

In their preliminary search, staff found virtually all personnel records contained information about other individuals—names, Social Insurance Numbers and other personal details—often in the form of lists, but also overtime sheets, payroll deduction lists and other memos and forms. Much of it concerned people no longer employees or who were not being transferred and, therefore, was irrelevant to NAV CANADA. And, of course, the individuals had not consented to the disclosure. Transport Canada agreed to remove the irrelevant material.

It also agreed to destroy many documents kept in personnel files and managers' working files long after they served any administrative purpose and well past the normal retention schedule. These included old disciplinary actions, resolved grievances, pay and tax forms, information about family-related leave and physicians' certificates to support employee sick leave.

Rating files in the Quebec region also included the employees' conflict of interest declarations and post-employment code attestations, neither of which apply to NAV CANADA. And the Cornwall Training Institute files held information on both successful candidates and others who failed or abandoned courses (many of them not ANS employees), some of it dating back to 1959. All this information has been removed and given to Transport's information management directorate for proper storage or destruction.

The result: Transport staff removed almost one million pages of outdated or irrelevant personal information from the files being transferred. That's 330 standard file boxes that, stacked one on top of the other, would reach 32 stories high. If nothing else, NAV CANADA records managers should be grateful.

The audit also identified personal data on ANS desktop computers, 3,500 of which will be transferred to NAV CANADA. Managers who maintain employment records in these computers were asked to remove the data of those not transferring. Transport Canada will define limits for access to mainframe computers and networks while NAV CANADA and Transport employees temporarily share offices and computer systems.

NAV CANADA has now received the personal information it needs on employees who accepted its offers of employment. Transport Canada will retain all other personnel files of employees who refused consent to the transfer, as well as outdated and other personal information that was removed from the files.

The good news: a sizeable chunk of Transport Canada files (and virtually all NAV CANADA personnel files) have had a thorough housecleaning. Perhaps the results will encourage the department to review the rest. Some of the problems Transport Canada encountered could have been minimized or avoided had NAV CANADA been made subject to the *Privacy Act*. Waiting until the privatization process was well under way before dealing with the privacy issues further exacerbated the problem. Involving the Commissioner's Office in the process from the outset is one solution but, ultimately, binding these new entities to the *Privacy Act* is a far better one.

Canada Student Loan Program

The program is one of those administered by Human Resources Development Canada. It now provides interest rate subsidies to financial institutions for loans to qualifying students but does not guarantee repayment of loans approved since the new *Canada Student Assistance Plan* took effect. Loans made under the previous *Canada Student Loan Act* will still be guaranteed by the federal government. In both cases, defaulted loans may eventually be given to collection agencies for recovery.

The audit reviewed the public listings in *Info Source*, information sharing, staff awareness of privacy protection, contracting out, security, use of telecommunications to transmit personal information and computers to process and store the data.

The Privacy Commissioner's staff suggested some minor adjustments (which they will follow up) but identified no substantive privacy weaknesses. They concluded that an intensive audit was not warranted, particularly given the government's diminishing role in loans written under the new program.

RCMP Public Complaints Commission

The Commission is an independent agency which reviews the RCMP's investigation of complaints against its members. It may also receive complaints directly from the public, although these too are referred to the RCMP for investigation. The Commission has regional offices in Vancouver and Edmonton but all complaint reviews are conducted at the Ottawa Head Office.

Privacy staff found the Commission generally in compliance with the *Privacy Act* but recommended it:

- seek consent to disclose in its reports personal information that is more than required to properly report the investigation;
- amend the personal information bank description to better describe the holdings and the retention and disposal schedules;
- destroy employment files of former employees held past the approved retention schedule, and evaluations of current employees held past the five-year period, and
- retain Members' notes as part of the Commission's information holdings.

The recommendation to retain members' notes could be affected by the Federal Court of Appeal decision in the case concerning access to notes of Canada Labour Relations Board members (see page 40).

Notifying the Commissioner

Designating a new "investigative body"

The Justice Department sought the Commissioner's views on designating Fisheries and Oceans' Conservation and Protection Directorate as an "investigative body" under paragraphs 8(2)(e) and 22(1)(a) of the *Privacy Act*.

The effect of this designation is to allow the body to withhold personal information from the individual for up to 20 years if it has been collected during "a lawful investigation", regardless how trivial, or whether disclosure would harm the investigation. In the legal jargon, this is a "class" exemption which—for the organization, at least—has the advantage of not obliging staff to review the files in response to an access request. Nothing need be released.

The Commissioner's response minced no words. Acknowledging that an individual's right of access had to be balanced against the state's need for secrecy, nevertheless he found it "unacceptable for this principle to find expression in any statutory provision that does not contain an injury test". He described section 22(1)(a) as "repugnant".

Despite the favourable findings of a 1996 Justice Department study into departments' use of 22(1)(a), the Commissioner observed that discretion in applying the blanket exemption is too rarely used. He cited examples of exempted files containing newspaper clippings, and correspondence between the department and the subject. While it may be simpler to apply 22(1)(a), "I do not believe that administrative convenience should be a consideration...".

The specific case was "particularly troubling" because the department's request had focused on making the case for similar exemption under the *Access to Information Act*. While there may be good reason for a class exemption from a general right of access under the Access Act (a matter for the Information Commissioner to consider), the application had failed to demonstrate the need to withhold an individual's own personal information under the *Privacy Act*—one would argue, a more onerous test. Certainly exemptions should not be invoked without considering the individual records and assessing what, if any, harm their disclosure might cause.

The department is reported to be pursuing the application which the Commissioner will continue to oppose.

“Public interest” disclosures

Although the *Privacy Act* generally prevents government departments and agencies from releasing clients’ and employees’ personal information, it lists several circumstances which may warrant disclosure. One of these, subsection 8(2)(m), permits the head of an organization to release information if he or she judges the public interest to outweigh any invasion of privacy. The head must then notify the Privacy Commissioner who may notify the individual(s) concerned, if he considers it appropriate.

Traditionally the heaviest users of this provision have been Correctional Services Canada, National Parole Board, and the RCMP—Correctional Services and the Parole Board to release reports on incidents involving inmates and parolees, and the RCMP to notify communities about impending release of a dangerous offender.

The number of notifications dropped slightly this year to 63 from 69, due mostly to fewer CSC notices. However, RCMP notifications increased to 12 from three last year, an increase due in part to delegating authority for these disclosures from headquarters to divisional commanders, and in part to a growing public outcry about public safety.

Nine of the notices concerned release of violent offenders in Manitoba communities following review by the new Manitoba Community Notification Advisory Committee. The RCMP has established its own policy on notifying communities about the arrival of violent or dangerous offenders, and several provinces have, or are about to establish committees to examine these notifications more systematically. For more information on these disclosures, (see page 35).

Other Matches

Office staff also reviewed two other data matching proposals, one of which—the HRDC student loan match—is ongoing.

Human Resources seeks student loan defaulters In another attempt to ferret out those who owe money to the government, Human Resources Development Canada (HRDC) asked Public Works and Government Services to match its list of student loan defaulters against the federal government employee database. Public Works approached the Office about the request.

Privacy staff pointed out that although Public Works administers the lists to provide pay and benefits services, it does so on behalf of Treasury Board which is

the public service employer. The Board is the real owner of the data and would have to agree with HRDC in order to submit a matching proposal. Despite its repeated verbal assurances that the Board agreed, HRDC was unable to produce written authorization. The Commissioner's Office would not consider the proposal without the Board's agreement and there the matter hung at the end of the reporting year.

Agriculture Canada sets off farmers' debts against benefits

Agriculture Canada proposed to match landowners' applications for benefits from two programs—the Arable Acres Supplementary Payments Program and the Freight Costs Pooling Assistance Program—against lists of farmers owing money to other Agriculture and Agri-Food Canada and Canadian Wheat Board programs. The cost-benefit analysis identified approximately \$900,000 as the amount to be recovered and the costs to be negligible as the computer software is already configured to run the match.

The match is not described specifically to Arable Acres Program applicants, however, Agriculture staff argued that “set-offs” are described as conditions of the program in both the application form and letter setting out the outstanding balance owing.

At one point it appeared that Agriculture was contemplating extending the match to other departments to which moneys are owed—apparently including Revenue Canada and Veterans Affairs. The Office could accept the specific match within the department as a consistent use of the information, but not an extension to other unrelated departments. Agriculture staff understood and the data matching proposal they eventually submitted was limited to the specific proposal.

Investigations Branch

Complaint intake surged ahead this year setting yet another record—2,235 received compared to 1,625 last year and the 1700 forecast. Investigators also completed 2,717, made possible by a combination of factors; a fast track process, a one-time infusion of funds from Treasury Board to hire contract staff (the money, and staff, are now gone) and internal re-alignment of staff. As well, one complainant withdrew 248 complaints, effectively freeing up two investigators.

The huge intake hampers the Office's efforts to substantially reduce its open caseload, investigators habitually carry an average of 90 open complaints at any given time—an excessive case burden. Too much investigator time is spent managing files and placating complainants. Caseload, inadequate resources, and government cuts in ATIP units, continue to seriously slow the entire process.

Delays In fact, delays have become endemic in some departments, due to the volume and increasing complexity of applications, and staff cuts. The seed of the problem was sown in 1983 when departments were told that there would be no new resources to handle requests under the then-new Privacy and Access to Information Acts.

Since then, federal agencies have responded to more than 650,000 applications as resources have been steadily cut. Unless technology-driven, there are no funds available and this work is people-intensive. Managers can only increase efficiency to a point—after that functions must be delayed, cut back or cut entirely. The ATIP program, not the core function of a department, is often high on the cut list. The result; service suffers, so too do the legitimacy and the credibility of the program.

Identifying Access Requesters Once again, the Office has grappled with the vexed question of whether identifying those who make *Access to Information* requests to other staff within the department or agency is a privacy violation. There is an understandable fear of chill—an apprehension that identifying the applicant could colour the department's response. Those looking for a simple answer will be disappointed.

Investigators have found some instances of departments routinely sending copies of the access request (which identifies the applicant) to program staff for a response. In some cases these staff had been delegated responsibility to approve the response, or to deal directly with the applicant to clarify points or simply to speed up the process. When this was not the case, the Commissioner has found the disclosure offends the *Privacy Act*.

As a general rule, the applicant's identity should not be revealed to other staff who do not need it in order to handle the access request. There may be other circumstances in which the disclosure of the applicant's name is justified. However, the Office recommended that departmental coordinators consider the circumstances of each application carefully to reduce the suspicion that the department is manipulating its response.

Streamlining the Investigation Process The Office continues reviewing and streamlining its own processes. During the year it re-grouped the branch into two units; one investigates complaints about government collection, use and disclosure of personal information, the other, all access-related complaints. It also implemented a "fast-track" system to reduce both the administrative and paper burden and elapsed time; established quality service standards to reduce the resources and turnaround time, improve the quality of the investigations and ensure more consistent findings; conducted in-house training to ensure consistency and enhance investigative skills, and transferred the Inquiries function to the Public Affairs unit to allow Branch management to concentrate strictly on complaint investigations.

Reducing the Backlog In an effort to reduce the backlog of cases—1629 carried over from the previous year, the Office has identified all files more than twelve months old (578 complaints or 35 per cent of ongoing cases), established a Backlog Unit which completed 375 investigations or 65 per cent of total backlog by the end of 1996, deployed other professional staff to finalize investigations—completing 38 complaints or 18 per cent of the 578 total; assigned virtually all time limits complaints to one junior privacy officer—closing 426 cases, thus freeing up senior investigators for more complex cases.

While these measures substantially reduced the number of cases open between six months and two years, the record intake of new complaints has simply shifted the indigestible chunk into the six to 12-month age bracket.

Cases

Covering Commissions of Inquiry

One complaint about disclosures of personal details during the Somalia Inquiry revisits a matter about which the Commissioner made recommendations in earlier annual reports—that commissions be added to the schedule to the *Privacy Act*. In this case, the inquiry ordered National Defence to turn over virtually all information considered relevant to the public inquiry including, obviously, large amounts of personal information.

DND was legally obliged to provide the material and the *Privacy Act* permits disclosures to comply with warrants or subpoenas. The Commissioner concluded that DND had not improperly disclosed personal details. But he and National Defence staff were concerned that an individual's control over the information is lost once in the hands of the commission of inquiry.

The Somalia commission assembled more than 100 Document books for legal counsel and the parties to the inquiry. Once filed as exhibits, the books are available to the media. The inquiry staff were conscious of the privacy implications of releasing the material and attempted to remove what it considered any irrelevant details. However, they are under no legal obligation to do so, thus privacy protection will vary from inquiry to inquiry, depending on the knowledge, time and inclination of staff.

Making commissions of inquiry subject to the *Privacy Act* would not impede their work; the act permits disclosures when the public interest "clearly outweighs any invasion of privacy that could result". But it would require commissions to consider carefully what disclosures clearly serve that public interest, and it would provide framework for access, disclosure and retention of inquiry material once the inquiry completes its work.

Canada Post spells out opt-out of Change of Address notices

This year the office concluded lengthy negotiations to attempt to resolve two complaints about Canada Post's change of address service.

The service redirects mail from clients' old to new addresses when they move (for a fee). Canada Post operates on cost recovery so it offers an address correction service to commercial and government mass mailers which (also for a fee) updates their clients' addresses, unless the client actively objects.

The complainants objected to the feature on the Change of Address Notification form telling clients that by signing the form "you consent to the information being provided, for address correction purposes, to mailers having your name and old address". More detail was provided in some accompanying material which the complainants argued was likely to be missed or thrown away in the pressure of moving. Assuming clients have given their permission if they are not heard from is a common commercial practice known as "opting-out".

Although technically speaking, there had been no improper disclosures (the complainants had opted out) the investigator took up the procedure with Canada Post. As part of its modifications to the Change of Address program, Canada Post agreed to provide more detail on the form itself and a toll-free line for clients to call if they have questions.

The Commissioner has made no secret of his dislike of opt-outs as a means of obtaining permission. Canada Post argues that the form is already too full to allow for a consent box and they are under some pressure from clients who frequently complain if they do not receive all their mail at their new addresses.

Anyone planning a move who objects to their new address being given to mass mailers should read the form carefully. Anyone who wants to reduce the amount of marketing mail can also use the Canadian Direct Marketing Association's *Do Not Call/Do Not Mail* service at

1 Concorde Gate, Suite 607
Don Mills, Ontario
M3C 3N6

Guidelines on using program files for employee supervision

Some government managers have to wear two hats when dealing with employees; one as employer and the second as program administrator. Distinguishing between the two functions and dealing with the person appropriately can pose a challenge. Following a complaint in 1993, Revenue Canada issued guidelines on using taxpayer information for monitoring or disciplining its employees; this year a similar complaint led Human Resources Development Canada (HRDC) to agree to do the same.

At issue was the employer's investigation of a woman's employment insurance (EI) claim file which was then used to discipline her as an employee. The woman, an insurance agent with the former Employment & Immigration Department (now HRDC) developed severe health problems and eventually used up her sick leave. Once her leave was gone, she applied for and received EI benefits.

To speed up her payments, she hand delivered her claims, and those of her son, directly to co-workers for manual input to the system. Although caught, suspended for eight days and counselled for the conflict of interest, she repeated the behaviour. Departmental managers became concerned about her pressure on co-workers in general, particularly on one in a trusted position, and examined her EI file. Her employment was terminated with an out-of-court settlement.

The woman complained that HRDC's use of her EI benefits file for employment purposes violated the *Privacy Act* because it meant using information gathered for one purpose—to pay her EI claim, for an unrelated use—disciplining her as an employee.

The department argued that the *Privacy Act* allows disclosures specified in other acts of Parliament and that it gathered the information to administer and enforce the EI Act, an essential component of which is to ensure the professionalism and personal integrity of the staff responsible for administering the program. Officials also maintained that the use was "consistent with" the original purpose for collection—to administer the EI act. The *Privacy Act* allows consistent uses.

The Commissioner rejected the proposition that the section of the EI act on which the department was relying (section 96) was anything other than a confidentiality provision to ensure that EI information was not disclosed outside the department. During a subsequent meeting to resolve the disagreement, privacy staff suggested HRDC examine the guidelines put in place by Revenue Canada to deal with similar extraordinary situations; examining an employee's income tax return.

At issue is not whether a department can discipline its employees for conflict of interest or other infractions, but ensuring that program files do not become a routine part of employee supervision. The circumstances which justify this use of non-employment information should be serious, the access restricted and the authority clear.

Office staff offered their advice and support in drafting appropriate controls. The department agreed and the Commissioner looks forward to seeing the results.

RCMP's disclosures during investigation "excessive"

A complaint from a lawyer challenged the information the RCMP revealed to several organizations about his client whom it was investigating. He argued the disclosure was excessive and in violation of the *Privacy Act*.

In an attempt to gather evidence for an investigation into alleged fraud and misappropriation of federal funds, the RCMP wrote to nine organizations seeking copies of any contracts they entered into with the individual and details of any disbursements they made. The letters disclosed information about the investigation, in particular that "evidence uncovered to date is overwhelming and prosecution will be unavoidable". The individual also complained to the RCMP Public Complaints Commission.

The RCMP should be able to demonstrate that its disclosures of personal information during investigations are required to fulfil its law enforcement and investigation mandate. During the Public Complaints Commission investigation, the RCMP acknowledged that the reference to the prosecution was unnecessary and apologized to the complainant for any discomfort this may have caused. Thus, by its own admission, the disclosure was excessive.

The privacy investigator reviewed the files, located the letter but could not find the same or similar statement in any of the preceding volumes. The comment first appears in the letter and seems to be the opinion of the writer. The RCMP agreed that the statement was unnecessary, improper and “lacking in tact”. The RCMP Commissioner undertook to ensure that proper training is available to all members who must secure evidence from outside bodies during economic crime investigations.

The Privacy Commissioner concluded that the complaint was well-founded but regretted that nothing further could be done to remedy the situation.

HRDC disclosures to private training companies tightened

One of the most immediate and visible signs of contracting out government services is the training courses offered employment insurance claimants. The courses, once given by Human Resources Development Canada, are now contracted out to private training organizations. This often comes as a surprise to the claimants who wonder where the company got their information.

A case in point was an Alberta woman who left her job to accompany her husband who was attending university in another city. She applied for employment insurance two weeks before the move and gave her new address. Shortly after moving she received a call from a company offering her a three week course, paid for by the department, on “employment issues”. Taken aback, she asked how they got her information and whether they were a private company. The company explained its status and role but the woman was “astounded” at the disclosure of the information outside the department.

The *Employment Insurance Act* allows the department to disclose information to “persons as the Minister deems advisable”. The investigator confirmed that the then-minister had signed an authorization to release information to contractors for purposes specified in the contract. The department had entered into a contract with the company which had called the complainant to provide training.

In an attempt to increase participation in the training, the department gave the names and telephone numbers of targeted EI applicants to the company which would market the course directly to applicants. The department did not tell the applicants or ask their consent for the disclosure and there was no mention of it in the supporting materials. The course was voluntary and the woman was not interested in its content, the focus of which was to help EI recipients deal with the personal changes, brought on by job loss that “negatively impact on their ability to become re-employed”. Since the training was not mandatory and the contract did not permit disclosure of personal information for marketing the course, the Commissioner concluded that the woman’s complaint was well-

founded. The investigator also found that the contracts contained no clauses protecting the personal information once in the hands of the company.

As a result of the woman's complaint, the Canada Employment Centre now consults clients before giving their names to private contractors for training. The description of the information and its uses in *Info Source* will be amended, and the EI application form has been changed to describe the potential use of claimant's information for training purposes. And, most important, Employment Centres have been instructed to ensure that contracts now contain clauses to protect clients' personal information. With these steps, the Commissioner considered the complaint resolved.

Lost file prompts new tracking system

A Second World War veteran's request for his medical file to support a disability pension application revealed that the file was apparently lost. When neither National Archives (which stores all old government personnel and military records) or Veterans Affairs could find the file, he complained to the Commissioner.

The veteran's original request went to Veterans Affairs. Since the file was more than two years old, the request was transferred to National Archives. Archives found the file was missing but did have a copy of a form indicating that it had been loaned to Veterans Affairs in 1987. Apart from keeping the form, Archives had no process to follow up and ensure that the file had been returned.

Veterans Affairs normally photocopies original files in Ottawa, returns the original to Archives, and forwards the copies to the appropriate regional office. It too found no trace of the file and believed it had been returned. Although a computerized system now tracks files borrowed from and returned to Archives, it was started in 1991. Any paper records from 1987 would have been destroyed as part of normal record review and destruction.

When the complainant produced a letter from the Royal Canadian Legion stating that staff had reviewed his file in 1988 to help him with his pension application, the investigator contacted the Legion. The Legion was happy to try to help but it was apparent that its staff only review original documents on site in government offices and take copies of the needed documents; they do not receive originals. Fortunately the copies they had taken were helpful. The investigator followed another possible lead to the Surgeon General's office at National Defence but it too was cold.

The investigator had to conclude that the file was gone or misfiled in Archives' huge inventory and too much time had elapsed for there to be any hope of

finding it. Had Archives file loan controls been better, the loss would have been noted much earlier and the chances of recovery far greater. Although little could be done to solve the immediate problem, the Commissioner wanted some assurance that the incident would not be repeated.

The investigation led Archives to initiate a file recall system for loans to other departments. The departments will now receive a formal recall notice at 90 days, and at 120 and 180 days if there are valid reasons for keeping the file longer than 90 days. The Commissioner concluded that the complaint against Archives was well-founded but, with the file recall system, now resolved. He dismissed the complaint against Veterans Affairs.

Complainant was source of personal details

It is evident that people often don't understand the implications of borrowing money and the collection and disclosure of personal information that is an integral part of the process. A man complained that a letter to him from a law firm about his unpaid Canada Student Loan contained information about his defective heart condition and his Social Insurance Number. He wanted to know how they got the information.

The man had defaulted on the loan and Human Resources Development Canada (HRDC) turned the matter over to a collection agency—the law firm. The firm obtained a credit report from Equifax (a major credit bureau) which contained the medical information, the name of his doctor, and the notation that the information was provided by the man himself during an interview.

Student loans are like commercial loans. The student borrows the money from a financial institution and authorizes the lender to exchange with credit bureaus, credit granters and credit reporting agencies information about the loan. This is part of the bargain between borrower and lender. The student loan program acts as guarantor for the bank. If a student defaults, the bank is paid by the government which then attempts to recover the money owing.

The law firm was acting as the department's agent in its attempt to get the loan repaid and had a legitimate reason to obtain the credit report from Equifax. In fact, the law firm acted in the complainant's interest when it explained to him that HRDC might defer its collection if he could provide information to confirm that his disability prevented his working and therefore repaying the loan.

The department also demonstrated that the Canada Student Loan Program is one of the federal activities legally mandated to use the SIN and, as its agent, the law firm had a right to it. The SIN was also in the man's Equifax file. Use of SINs by credit agencies is the single biggest motivator for private sector requests for

the number and is outside of the federal government's jurisdiction. The Commissioner dismissed the complaint.

Should employees expect privacy for their e-mail?

An employee of a Correctional Service Canada (CSC) treatment centre alleged that the secretary of the division had obtained her computer password and accessed her e-mail without consent during her absence. She complained that the access breached her privacy and that of inmates whose personal information was in her data base.

The investigator established that CSC headquarters had called for a copy of a document the complainant had prepared but it had not received. The request was urgent, the complainant was absent but her secretary knew it had been sent and could be found in her e-mail. She asked the divisional secretary for help. Informatics staff suggested re-setting the complainant's access code to allow the secretary to obtain the document. The Assistant Warden gave the secretary permission to re-set the code in order to access the e-mail.

The complainant argued that a copy could have been obtained from another office. She suspected that her supervisor wanted access to her communications with a union representative and another employee concerning her harassment complaint against him. In fact, only her secretary entered her computer and she insisted that she did not browse through the e-mail or any personal files. She knew approximately when the e-mail had been sent and found it quickly.

The investigator found no evidence that there had been any improper disclosure of personal information. Computer passwords are the equivalent of locks and access lists for conventional paper records; they are to prevent unauthorized access by individuals who have no need to examine information in employees' working files. However, no matter the medium, information employees prepare for government business and stored on government premises should be available to an individual's supervisor if there is a demonstrated need during an employee's absence.

The Commissioner agreed with the complainant that access should always be controlled and authorized by the employee's supervisor. As a result of the complaint, CSC informatics staff now require a written authorization from a supervisor before re-setting passwords.

Managers and employees alike should remember that e-mail is not secure and even deleted e-mail messages can sometimes be retrieved. In short, these systems should not be used to send or store anything they don't want others to read. The complaint was not well-founded.

Tax reassessment of travel allowances no “fishing expedition”

Several RCMP members complained to the Commissioner that by giving Revenue Canada a list of those receiving transfer allowances from 1991 to 1993, the RCMP had improperly disclosed personal information. (They also complained about Revenue Canada’s collection of the information.) The complainants argued that the request was akin to a “fishing expedition” and that Revenue Canada was obligated by the *Income Tax Act* to obtain a judge’s order to obtain information about unnamed individuals, and the RCMP should not have relinquished the list without one.

At issue is the allowance paid to RCMP members when transferred to a new location. The allowance, equal to 1/12 the annual salary, is to be taxed at source by the RCMP and reported by members as a taxable benefit on that year’s income tax return. Members are told this when paid the allowance. In contrast, actual moving expenses are fully deductible with receipts.

A Revenue Canada audit of Regina District RCMP members revealed that many were simply deducting the full amount of the allowance as a moving expense. Auditors also discovered that the RCMP had not properly reported the taxable allowance on members’ T4 slips. If it had, Revenue Canada could have found any discrepancies from its own computer system and not needed the RCMP’s list. Once Revenue Canada discovered the omission, it asked the RCMP for the lists to conduct a random sampling to determine the extent of the problem. Following a telephone conversation between the RCMP Commissioner and the Revenue Canada Deputy Minister, the RCMP agreed to turn over the necessary records to ensure that transfer allowances were being properly reported.

Revenue Canada reviewed the computer tape and examined the returns of all members who received the transfer allowance during the three years at issue. Of the 1400 returns, 633 were reassessed and \$1,227,000 in unpaid taxes was recovered. The remaining returns were processed with no changes, either because the member did not claim the allowance or the return had already been re-assessed by a field office in the post-review process.

It was clear to the Commissioner that both departments were cognizant of the restrictions in both the *Privacy Act* and the *Income Tax Act*, had sought legal advice and proceeded carefully. The RCMP is required to report properly to Revenue Canada any benefits paid its employees. Rather than ask the RCMP to re-issue T4 slips to all its members for the relevant years (which would have triggered a review of every member’s file) Revenue Canada focused its request on a list of only those who had received the transfer allowance. The Commissioner concluded that Revenue Canada is entitled to collect the information under the *Income Tax Act* and therefore there was no violation of the *Privacy Act*.

Air crew remarks to safety inspectors given to airline

The disclosure of an employee's critical comments to the employer can have predictable consequences and require a careful assessment of whether the remarks are simply letting off steam, or information to which the employer is entitled. This was evident when the flight service director of an Air Canada cabin crew allegedly told a Transport Canada inspector that a number of the shortcomings she noted on the trans-Atlantic flight were due to the airline emphasizing service over safety. The inspector paraphrased all the crew members' remarks and relayed them to the airline in her report. The report led the airline to correct the deficiencies and to take disciplinary action against the flight director. He, in turn, complained that the inspector's disclosure was improper.

The investigator found that the inspector had noted numerous violations of the *Aeronautics Act*, *Air Regulations* and related Air Navigation Orders. Normally inspection reports are sent monthly to appropriate airline personnel. Only when inspectors note "extensive non-conformities" do they issue separate letters of finding. The inspector's letter noted both the specific violations and her interpretation of the flight director's remarks that the company should be blamed for the non-conformities, not him, since cabin crew had been complaining for some time about service considerations overriding safety procedures. The flight director said his comments had been misinterpreted.

Airline inspection personnel find interviews with flight crew a valuable source of information since crew often voice concerns to inspectors they would be reluctant to express to their employer. Open communication between inspectors and crew is essential. However, safety comes first. When inspectors find cabin crew not complying with safety requirements, they must report this to airline management. Management, in turn, must respond in writing to Transport Canada on its corrective action. As well, the flight director has overall responsibility for service, safety and cabin crew and is subject to disciplinary action when there are extensive violations. Although airlines usually determine the disciplinary action, Transport Canada can make specific suggestions and recommendations.

It was evident from the legislation, regulations and procedures manuals that Transport Canada has authority to inspect flight safety and communicate its findings, including relevant crew comments, to the airlines. The inspector considered the crew's comments were relevant to flight safety and required by the airline to correct the shortcomings. The Commissioner concluded that Transport Canada has clear legislative authority for safety inspections and that the inspector disclosed the crew's remarks for the very purpose for which they were gathered—to deal with safety violations. Thus there had been no violation of the *Privacy Act*.

Nevertheless, the Commissioner agreed that paraphrasing the crew's remarks risks misinterpretation, particularly when the crew does not see the written report and thus has no opportunity to correct misunderstandings. The comments are often gathered while flight crew are busy on descent which may prompt less than careful remarks. The Commissioner recommended inspectors have an opportunity to share written findings with aircrew before submitting them to the airline. He also recommended inspectors make a greater effort to record the crew's comments verbatim to avoid misinterpretation.

Instructor circulates students' information

A student on a course at a private training centre under contract to Human Resources Development Canada (HRDC) complained that the instructor had circulated a list of the students' names, addresses, telephone numbers and Social Insurance Numbers for each student to verify the information. Circulating one list effectively disclosed her personal details to each of the other students. She thought there should be some penalty against the centre.

There was no doubt that the private training centre was under contract to HRDC and thus bound to respect the *Privacy Act*. Nor was there any dispute that the information had been disclosed. The investigator interviewed the instructor who confirmed that HRDC had advised her that she was responsible for protecting her students' personal information. She confirmed that the centre would use individual sheets in future.

The investigator explained to the complainant that there are no penalties against the training centre—HRDC is held responsible for the actions of its contractors. The complaint was well-founded.

Request for Archives investigation not "personal"

A letter asking the National Archivist to investigate allegations of improper document destruction at National Defence prompted a complaint from the writer that the letter should not have been disclosed to DND.

The letter set out the writer's allegations, named DND sources who could provide information, and asked the Archivist to investigate. Since National Archives does not have the power to enter a department and investigate on its own right, the Archivist wrote to the Deputy Minister of National Defence enclosing a copy of the letter, and asking him to investigate the allegations.

The complainant argued that the letter contained confidential and personal information, including the name of his sources, which should not have been disclosed, and that his own privacy had been violated by Archives' release of his letter to DND.

The Archives argued that the letter was on company letterhead and therefore did not appear to be personal, the writer had not asked for confidentiality (a request made—and respected—in an earlier letter), the Archivist could not investigate without the full cooperation of DND, and the department could not investigate without knowing the allegations against it.

The Commissioner concluded that the writer clearly wanted Archives to investigate and had provided the information in order for it to do so. Archives has no investigative power of its own and, therefore, it was reasonable that it should provide the allegations to DND for it to investigate. In effect, Archives used the information for the purpose for which it was provided.

It is also a fundamental principle of natural justice that an accused be able to face the accuser and know the charges being made. This is true even of complaints under the *Privacy Act*—the complainant's name and allegations are given to the department cited. The Commissioner considered the complaint not well-founded.

Inquiries

This year's inquiries exceeded 9600 for the first time. Inquiries range from straightforward questions about the *Privacy Act*, to how to get a pardon, remove names from mass mailing lists, or find natural parents. And each time the federal government launches a new program or begins another collection of personal information—the last census, the Consumer Price Index survey, or matching Customs and EI data—the telephones start to ring.

A substantial segment of the work deals with referring callers to organizations which may be better placed to help. Clearly a number of callers are frustrated to discover the limit of the Commissioner's mandate and angry that, in fact, there is no legal protection for their privacy. We encourage them to support the government's initiative to have national privacy legislation in place by the year 2000.

About 40 per cents of the inquiries are in the Commissioner's jurisdiction and focus on using and interpreting the *Privacy Act*. The next largest group, requests for Office publications and calls from the media, makes up 18 per cent. Referrals to our provincial counterparts count for eight per cent and complaints about uses of the Social Insurance Number seven per cent (see below). The remaining 27 per cent concern such issues as telemarketing and direct mail, adoption, geneology, credit reporting, financial institutions, and medical records.

Hydro Québec asks new customers for SIN

Many Canadians view the federal government as the custodian and supervisor of the Social Insurance Number, and the federal Privacy Commissioner as its national guardian. In fact, neither is true. The federal government has a strict policy on its own uses of the ubiquitous SIN but no power to control how others use it. A case in point is Hydro-Québec's request for SINs from new customers which prompted a deluge of calls demanding that the federal Commissioner intervene because it is a "federal number".

The Québec Information and Privacy Commissioner and Hydro-Québec (which is subject to the provincial privacy law) debated the issue at some length and appeared headed for court. By mutual consent both parties agreed to step back and find a solution with which both could live. Hydro-Québec convinced the provincial commissioner that using SIN was the only way to track down customers who move without paying their bills. The commissioner, in turn, got Hydro's agreement to create a new unique ID number from the SIN, remove some gratuitous personal details from its files and allow only its collection staff access to the actual SIN. In May 1996, the Quebec National Assembly passed Section 8 of Hydro-Québec By-Law 634 giving the corporation the right to request SIN from customers "opening an account". Once Hydro began advising its customers that it might ask for their SINs, the phones began to ring.

The federal Privacy Commissioner continues to object to compelling people to provide their SIN for uses completely unrelated to their original purpose. However, given that Hydro-Quebec's by-laws now require the SIN, its customers have no legal grounds for refusing.

New Permanent Register for Electors

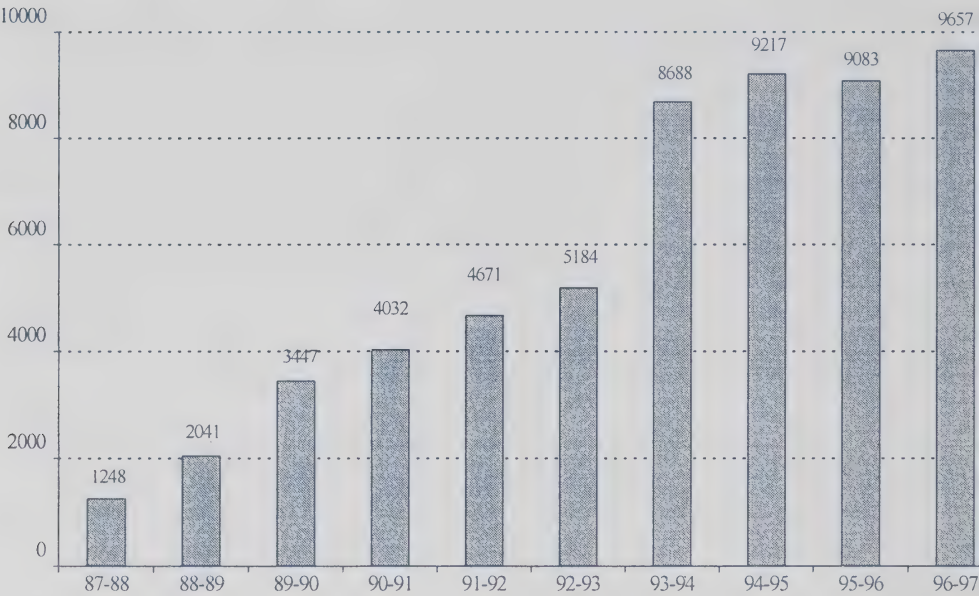
The office also received several calls from individuals upset with Elections Canada's request for their date of birth on the enumeration form for the new permanent voters register (see page 19 for more detail). Elections Canada collects the birth date and gender to help it distinguish between individuals with the same or similar names. The information does not appear on the lists given to political parties each year. Inquiries officers explain that the register is protected under both the *Privacy Act* and the *Elections Act* and voters do not need to be in the register to vote. Voters also have the right to withdraw their names or to prevent their transfer to the provinces or territories by writing to the Chief Electoral Officer.

Errors on credit files

We continue to receive many calls from individuals who are concerned about errors on their credit files. Credit bureaus in Canada are private businesses and therefore are not covered under the *Privacy Act*. They are regulated by

provincial consumer protection laws so the details of the parties' rights and responsibilities vary from province to province. Individuals who have not been able to have errors corrected by their local credit bureau should contact their provincial agency which administers consumer protection law.

Inquiries 1987-97



Top Ten Departments by Complaints Received

		Grounds			
Institution		TOTAL	Access	Time	Privacy
Correctional Service Canada		602	134	422	46
National Defence		389	93	267	29
Revenue Canada		215	70	89	56
Justice		208	101	97	10
Human Resources Development		141	53	38	50
Immigration and Refugee Board		115	65	38	12
Citizenship and Immigration Canada		110	66	38	6
Royal Canadian Mounted Police		86	57	2	27
Canada Post Corporation		69	37	7	25
Canadian Security Intelligence Service		45	44	1	0
OTHER		255	108	66	81
	TOTAL	2,235	828	1,065	342

Completed Complaints by Grounds and Results

Grounds		Disposition					TOTAL	
		Well-founded	Well-founded; Resolved	Not Well-founded	Discontinued	Resolved		Settled
Access		20	77	468	234	69	261	1,129
	Access	20	76	443	227	62	227	1,055
	Correction/Notation	0	0	25	5	4	32	66
	Inappropriate Fees	0	1	0	2	0	1	4
	Index	0	0	0	0	1	0	1
	Language	0	0	0	0	2	1	3
Privacy		46	39	183	98	11	83	460
	Collection	3	0	54	19	4	25	105
	Retention & Disposal	11	12	20	8	2	6	59
	Use & Disclosure	32	27	109	71	5	52	296
Time Limits		704	0	274	136	1	13	1,128
	Correction/Time	7	0	5	4	1	6	23
	Time Limits	690	0	109	129	0	7	935
	Extension Notice	7	0	160	3	0	0	170
TOTAL		770	116	925	468	81	357	2,717

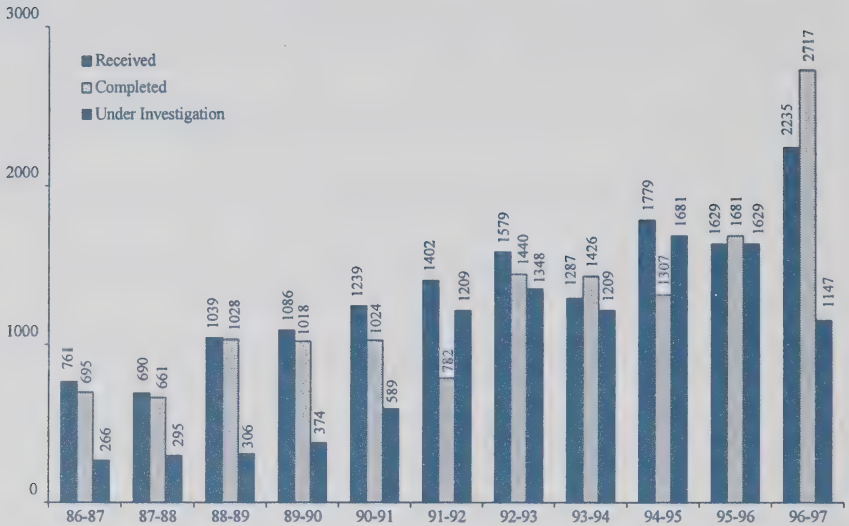
Completed Complaints by Department and Result

Department	Total	Well-founded	Well-founded; Resolved	Not well-founded	Discontinued	Resolved	Settled
Agriculture and Agri-Food Canada	16	1	0	2	10	1	2
Auditor General of Canada	2	0	0	0	2	0	0
Bank of Canada	1	0	0	1	0	0	0
Business Development Bank of Canada	5	4	0	0	0	0	1
Canada Council	1	0	0	1	0	0	0
Canada Mortgage and Housing Corporation	5	1	0	1	2	0	1
Canada Ports Corporation	1	0	0	1	0	0	0
Canada Post Corporation	112	5	5	71	9	10	12
Canadian Environmental Assessment Agency	1	0	0	1	0	0	0
Canadian Heritage, Department of	8	0	1	1	5	1	0
Canadian Human Rights Commission	18	1	3	11	0	1	2
Canadian International Dev. Agency	1	0	0	0	0	1	0
Canadian Radio-Television and Telecommunication Commission	3	0	0	3	0	0	0
Canadian Security Intelligence Service	73	0	3	52	4	1	13
Canadian Space Agency	22	0	0	18	0	4	0
Citizenship and Immigration Canada	122	39	8	37	11	4	23
Correctional Service Canada	731	293	24	269	50	19	76
Environment Canada	19	0	9	8	0	0	2
Farm Credit Corporation Canada	6	0	2	2	0	0	2
Fisheries and Oceans	11	1	1	1	0	0	8
Foreign Affairs and Int. Trade Canada	10	6	0	4	0	0	0
Health Canada	17	7	0	3	1	3	3
Human Resources Development Canada	176	35	24	45	25	8	39
Immigration and Refugee Board	93	54	1	15	21	0	2
Indian and Northern Affairs Canada	22	1	1	13	6	0	1
Industry Canada	12	0	0	5	3	0	4

Completed Complaints by Department and Result

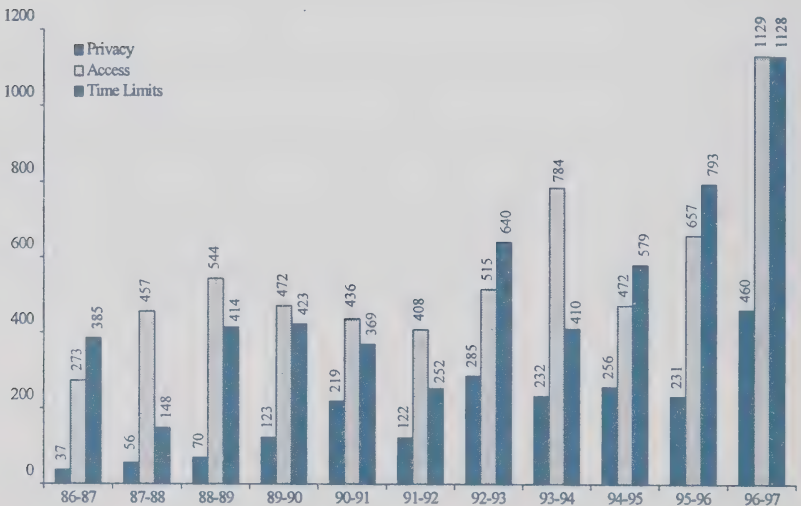
Department	Total	Well-founded	Well-founded; Resolved	Not well-founded	Discontinued	Resolved	Settled
Jacques-Cartier & Champlain Bridges Inc.	4	0	3	0	0	0	1
Justice Canada, Department of	209	2	1	20	179	5	2
National Archives of Canada	55	9	0	29	6	0	11
National Arts Centre	1	0	0	0	0	0	1
National Defence	429	187	10	79	90	1	62
National Library of Canada	1	0	0	0	1	0	0
National Parole Board	27	4	2	11	7	2	1
National Research Council Canada	1	0	0	1	0	0	0
Natural Resources Canada	4	0	2	1	0	1	0
Natural Sciences and Engineering Research Council of Canada	1	0	0	1	0	0	0
Privy Council Office	5	1	0	3	0	1	0
Public Service Commission of Canada	24	5	1	13	3	1	1
Public Works and Govt. Services Canada	11	1	0	6	2	0	2
RCMP Public Complaints Commission	15	0	0	5	0	1	9
Revenue Canada	231	100	7	74	17	7	26
Royal Canadian Mint	1	0	1	0	0	0	0
Royal Canadian Mounted Police	162	3	4	103	10	7	35
Social Sciences and Humanities Research Council of Canada	1	0	0	0	0	0	1
Solicitor General Canada	2	0	0	0	0	0	2
Statistics Canada	3	1	0	1	0	0	1
Transport Canada	31	9	2	7	4	1	8
Treasury Board of Canada Secretariat	6	0	1	3	0	0	2
Veterans Affairs Canada	4	0	0	3	0	1	0
Western Economic Diversification Canada	1	0	0	0	0	0	1
TOTAL	2,717	770	116	925	468	81	357

Completed Complaints 1986-97

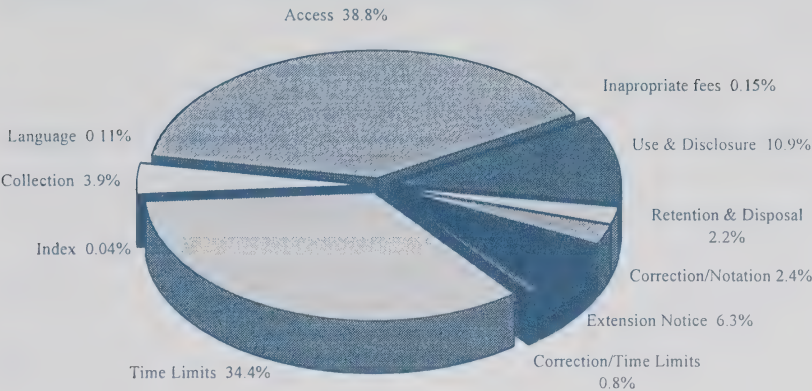


* The chart reflects minor adjustments to 1993-94 to 1995-96 count

Completed Complaints and Grounds 1986-97



Complaints Completed by Grounds



Origin of Completed Complaints

Newfoundland	13
Prince Edward Island	4
Nova Scotia	60
New Brunswick	68
Quebec	644
National Capital Region Quebec	36
National Capital Region Ontario	506
Ontario	646
Manitoba	54
Saskatchewan	88
Alberta	186
British Columbia	395
Yukon	5
Northwest Territories	1
Outside Canada	11
TOTAL	2,717

International Privacy Commissioners Meet in Ottawa

Last September, the Office hosted the 18th International Data Protection Commissioners Conference in Ottawa. The conference, which began as an informal annual meeting of Western European data protection and privacy commissioners, has evolved into an event to exchange information and examine the privacy implications of new trends, techniques and technologies.

The 1996 conference attracted 300 provincial, territorial and foreign commissioners and for the first time a large contingent of government and industry representatives and privacy protection advocates from around the world. The commissioners represented 23 countries and 17 sub-national jurisdictions (for example, Canadian provinces and German states).

The 1996 Ottawa conference theme, *Privacy Beyond Borders*, focused on the privacy impact of growing international trade in personal information. The Ottawa conference offered the first opportunity to attract a sizeable North American contingent, as well as participants from other countries interested in the North American approach to data protection.

The first two days of the three day conference were open to all participants and consisted of presentations and panel discussions. The last day was a business meeting for privacy commissioners and their staffs to exchange views on administrative, legal and policy issues common to their operations. Among the topics debated at the public meetings were:

- the new European Union Directive on the protection of data and privacy, and its impact on North American businesses;
- increasing surveillance of individuals, including workplace monitoring and the use of information relating to a person's whereabouts;
- international developments in data protection and privacy legislation; and
- privacy and selected Canadian private sector industries.

These annual conferences serve many purposes, most important of which is sharing experiences with privacy issues that increasingly respect no national boundaries. Canada can learn much from other countries' privacy initiatives, and our own privacy bodies have much to share with other jurisdictions. In an environment in which increasingly scarce public resources are being shifted to programs and systems that threaten to erode privacy, few are available for its

protection. The data protection commissioners conference offers the prospect of some synergy.

Many of the papers presented at the conference are available on our Internet web site at <http://infoweb.magi.com/~privcan/>. The office also has available a limited number of bound copies of the papers.

Privacy Protection In Canada...an update

British Columbia will begin reviewing its *Freedom of Information and Protection of Privacy Act* later this year. The Legislature is expected to appoint a Special Committee that will report back to the Legislative Assembly within one year on the results of its review, including any recommended amendments.

There was some concern that the government might amend the act before the committee completed its review. The government now appears to have postponed any such plans and will allow the committee to hear representations before considering any changes.

Alberta introduced Bill 1 to extend the *Freedom of Information and Protection of Privacy Act* to schools, health authorities, post-secondary institutions and municipalities. The bill allows local public bodies to be phased into the act, sector by sector, as they are ready. The education sector is expected to be the first new group brought under the legislation, followed by the health sectors and the municipalities.

The government also released a discussion paper entitled *Striking the Right Balance* as part of the process of preparing new health legislation. At issue is the balance between sharing information to improve health and health care while protecting the privacy of an individual's personal health information. Results of the consultations will lead to draft legislation to be introduced later in 1997.

Manitoba is planning to table a new freedom of information and protection of privacy bill to replace the 1988 *Freedom of Information Law* which deals only with access to personal records. The new bill would include a fair information code—rules for government collection, use and disclosure of residents' personal information. It would also address the impact of growing application of electronic technology on information rights.

In addition, the province is considering a separate medical privacy protection bill to strengthen health privacy provisions across many different statutes, and to respond to growing concerns over protecting personal health information with the advent of new health information-sharing technologies.

In July 1996, the **New Brunswick** Ministry of Justice released a discussion paper seeking comments on a proposed *Privacy Act*. This new law, somewhat similar to the federal law, would replace the December 1994 voluntary Privacy Code and apply to provincial government records. Like the code, the law would be overseen by the province's Ombudsman.

The **Northwest Territories'** *Access to Information and Privacy Act* came into force in January 1997. In anticipation of the April 1999 splitting of the Territories to create Nunavut, however, minor changes were made to the law before it came into force. The Information and Privacy Commissioner will be a private sector specialist instead of a government employee, and his/her term will end in March 1999.

In March 1996, the **Nova Scotia** advisory committee reported on its review of the province's 1993 *Freedom of Information and Protection of Privacy Act*. The committee made 65 recommendations including extending the act to private businesses under contract to the provincial government, to academic institutions, and to municipal and regional agencies, and appointing a commissioner to replace the existing part-time Review Officer.

Ontario's February 1996 omnibus bill brought changes to its *Freedom of Information and Protection of Privacy Act*. Applicants must now pay a \$5 fee to examine their own information, and a further \$10 if they wish to lodge a privacy complaint with the province's Information and Privacy Commissioner. The Bill also allows an institution to refuse to respond to requests which the head has reasonable grounds to believe are "frivolous or vexatious".

Another bill amended the provincial law to remove from its application any records an institution collects, maintains or uses concerning communications, consultations, discussions, meetings, negotiations or proceedings about labour relations or employment-related matters in which the institution has an interest. These changes could deprive provincial employees of much of their right of access to, and correction of, their personal information.

Quebec's Bill 32, enacted in June 1996, somewhat weakened that province's privacy law by furnishing the provincial Ministry of Revenue unprecedented powers to obtain personal information from other provincial and municipal agencies to catch "tax cheats". The Ministry must notify the provincial Privacy Commissioner who will monitor but may not stop the collection. As well, Québec set up a province-wide prescription drug network which became operational in January 1997, stirring some privacy concerns. The province also announced that, beginning in 1998, it would replace existing health care cards with smart cards, although these would not contain a person's medical record but act as a key to centralized computer files. Lastly, Quebec's National Assembly held a series of public consultations in March 1997 on the need for a provincial identity or multi-purpose card. No recommendations have been made to the government to date.

Yukon has enacted a revised access to information law which now includes provisions for protecting territorial residents' personal information and privacy. The new law is overseen by the territorial Ombudsman, who doubles as Information and Privacy Commissioner.

Corporate Management

The Offices of the Information and Privacy Commissioners share premises and administrative support services while operating separately under their statutory authorities. These shared services—finance, personnel, information technology advice and support, and general administration—are centralized in Corporate Management Branch to avoid duplication of effort and to save money for both government and the programs. The Branch has just 15 staff and a budget of approximately 15 per cent of total program expenditures.

Resource Information

The Offices' combined budget for the 1996-97 fiscal year was \$6,657,000. Actual expenditures for 1996-97 were \$6,669,015 of which personnel costs—\$5,452,166, and professional and special services expenditures (contractors and outside legal counsel) \$721,248—accounted for more than 93 per cent of all expenditures.

The remaining \$495,601 covered all other costs including postage, telecommunications services, supplies, equipment, travel and printing for both programs, the 84 employees and two Commissioners.

Actual expenditure details are reflected in Figure 1 (Resources by Organization/Activity) and Figure 2 (Details by Object of Expenditure).

Figure 1: 1996-97 Resource Use by Organization/Activity

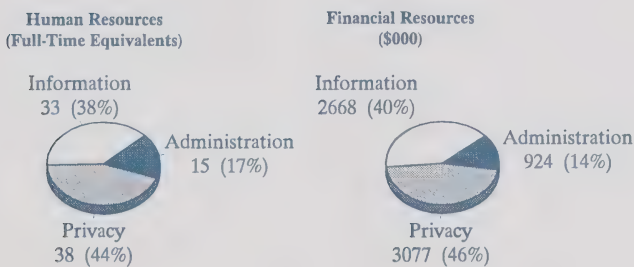
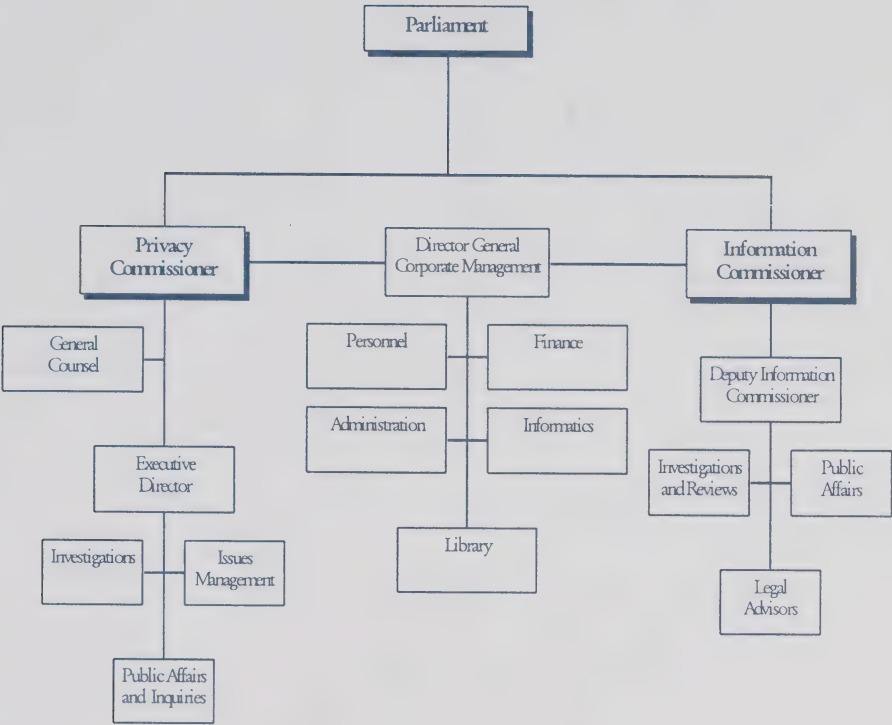


Figure 2: Details by Object of Expenditure

	Information	Privacy	Corporate Management	Total
Salaries	1,996,206	2,169,513	593,447	4,759,166
Employee Benefit Plan Contributions	277,000	323,000	93,000	693,000
Transportation and Communication	48,979	59,566	128,191	236,736
Information	23,531	66,867	2,010	92,408
Professional and Special Services	259,691	421,326	40,231	721,248
Rentals	3,863	14,316	14,653	32,832
Purchased Repair and Maintenance	12,515	2,130	7,356	22,001
Utilities, Materials And Supplies	30,418	13,042	35,738	79,198
Acquisition of Machinery and Equipment	15,105	5,693	9,335	30,133
Other Payments	655	1,122	516	2,293
Total	2,667,963	3,076,575	924,477	6,669,015

* Expenditure Figures do not incorporate final year-end adjustments reflected in the Offices' 1996-97 Public Accounts.

Organization Chart



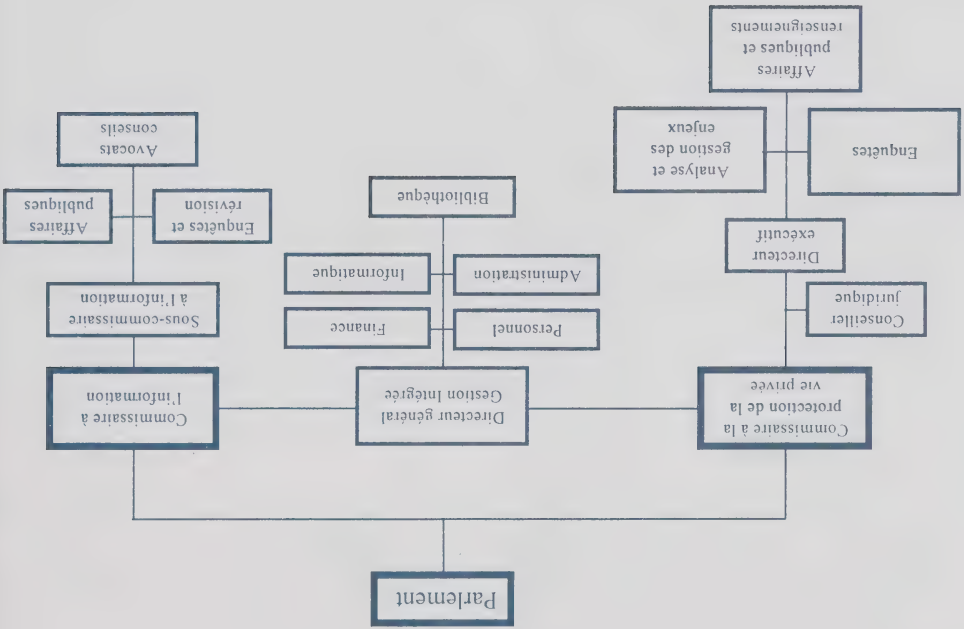


Tableau 1: 1996-97 Ventilation par organisme/activité

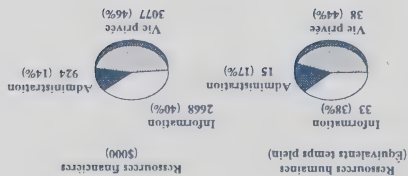


Tableau 2: Ventilation par type de dépense

	Information	Vie privée	Cession	Total
Salaires	1,996,206	2,169,513	593,447	4,759,166
Contributions aux régimes d'avantages sociaux	277,000	323,000	93,000	693,000
Transports et communications	48,979	59,566	128,191	236,736
Information	23,531	66,867	2,010	92,408
Services professionnels et spéciaux	259,691	421,326	40,231	721,248
Locations	3,863	14,316	14,653	32,832
Achat de services et réparations	12,515	2,130	7,356	22,001
Services publics, fournitures	30,418	13,042	35,738	79,198
Achat de machines et d'équipement	15,105	5,693	9,335	30,133
Autres	655	1,122	516	2,293
Total	2,667,963	3,076,575	924,477	6,669,015

* Ces dépenses ne reflètent pas les rajustements de fin d'exercice indiqués aux Comptes publics des Commissariats pour 1996-97.

Direction de la gestion intégrée

Par souci d'économies et d'efficacité, le Commissariat à la protection de la vie privée et le Commissariat à l'information partagent leurs locaux et leurs services administratifs. Les deux commissariats fonctionnent cependant de façon indépendante en vertu des deux lois habilitant leurs opérations. Les services administratifs sont assurés par la Direction de la gestion intégrée, et comprennent les finances, le personnel, les conseils et le soutien informatique, les télécommunications, la bibliothèque et l'administration générale. La direction a un personnel de quinze personnes et un budget qui représente environ 15 p. 100 du budget total des dépenses de tout le programme.

Description des ressources

Le budget combiné que les deux Commissariats avaient projeté pour l'exercice financier 1996-1997 s'élevait à 6 657 000\$. Les dépenses réelles pour l'exercice 1996-97 étaient de 6 669 015 \$. De cette somme, 5 452 166 \$ ont été affectés au personnel et 721 248 \$ ont été versés en services professionnels et spéciaux (contractuels et conseillers juridiques de l'extérieur), soit 93 p. 100 de toutes les dépenses.

Le solde, soit 495 601 \$ a couvert tous les autres coûts dont la poste, les frais de télécommunications, les fournitures, l'équipement, les déplacements et l'impression pour les deux programmes, les 84 employés et les deux Commissaires.

Les dépenses actuelles se retrouvent au tableau 1 (Ventilation par organisme et activité) et au tableau 2.

Le projet de loi 32 du Québec, adopté en juin 1996, a quelque peu affaibli la loi fournissant au ministre du Revenu de la province des pouvoirs sans précédent pour obtenir des renseignements personnels d'autres organismes provinciaux et d'organismes municipaux dans le but d'attraper les fraudeurs de l'impôt. Le ministre sera tenu de signaler son intention d'obtenir ces renseignements au commissaire à la protection des renseignements personnels, mais ce dernier n'aura pas le pouvoir d'arrêter la collecte des données. En outre, le Québec a mis sur pied un réseau provincial de surveillance des médicaments d'ordonnance, qui est entré en service en janvier 1997 et a suscité des préoccupations en matière de protection des renseignements personnels. La province a aussi annoncé qu'à partir de 1998, elle remplacera les cartes d'assurance-santé actuelles par des cartes à puce; toutefois, ces dernières ne renfermeraient pas le dossier médical d'une personne, mais seraient une clé donnant accès à un répertoire central informatisé. En dernier lieu, l'Assemblée nationale du Québec a tenu une série de consultations publiques en mars 1997 sur le besoin de créer une carte d'identité provinciale ou une carte à multiples usages. Aucune recommandation n'a été soumise à ce sujet au gouvernement jusqu'à ce jour.

Le Yukon a adopté une loi révisée sur l'accès à l'information, qui comporte maintenant des dispositions sur la protection des renseignements personnels et de la vie privée des résidents du territoire. La nouvelle loi sera surveillée par l'Ombudsman du Yukon, qui agira aussi à titre de commissaire à l'accès à l'information et à la protection des renseignements personnels.

renseignements médicaux personnels, attribuables aux nouvelles technologies d'échange des renseignements médicaux.

En juillet 1996, le ministre de la Justice du Nouveau-Brunswick a publié un document de travail dans lequel il sollicitait des commentaires sur un projet de loi sur la protection des renseignements personnels. La nouvelle loi, qui est semblable à la loi fédérale du même nom, remplacerait le code de protection des renseignements personnels, en date de décembre 1994, et s'appliquerait aux dossiers du gouvernement de la province. Tout comme le code, la loi serait sous la surveillance de l'ombudsman de la province.

La loi *Access to Information and Privacy Act* des Territoires du Nord-Ouest a pris effet en janvier 1997. Compte tenu de la séparation des Territoires pour créer le territoire Nunavut, en avril 1999, des changements mineurs ont été apportés à la loi avant son entrée en vigueur. Le commissaire à la protection des renseignements personnels sera un spécialiste du secteur privé plutôt qu'un employé du gouvernement, et son mandat se terminera en mars 1999.

En mars 1996, le comité consultatif de la Nouvelle-Écosse a signalé les résultats de son examen de la loi *Freedom of Information and Protection of Privacy Act* de 1993. Le comité a présenté 65 recommandations, comme d'étendre les dispositions de la loi aux entreprises privées qui ont signé des contrats avec le gouvernement de la province, aux établissements d'enseignement, ainsi qu'aux organismes régionaux et municipaux, et de nommer un commissaire pour remplacer l'agent d'examen, dont le poste est actuellement à temps partiel.

Le projet de loi omnibus de février 1996 de l'Ontario a entraîné la modification de la Loi sur l'accès à l'information et la protection de la vie privée. Un requérant doit maintenant déboursier 5 dollars pour consulter ses propres renseignements, et un autre 10 dollars s'il souhaite déposer une plainte en matière de vie privée auprès du commissaire à l'accès à l'information et à la protection de la vie privée de la province. Le projet de loi permet aussi à une institution de refuser de répondre aux demandes que l'administrateur de l'institution juge, pour des motifs raisonnables, à caractère frivole ou vexatoires.

Un autre projet de loi a modifié la loi provinciale, qui ne s'applique plus aux documents qu'une institution recueille aux fins de communications, consultations, discussions, réunions, négociations ou instances en matière de relations de travail, dans son domaine d'intérêt. Ces changements pourraient priver les employés provinciaux d'une grande partie de leur droit d'accès à leurs renseignements personnels et à la correction de ces renseignements.

La protection des renseignements personnels au Canada—mise à jour

La Colombie-Britannique commencera à réviser sa loi *Freedom of Information and Protection of Privacy Act* plus tard au cours de l'année. L'Assemblée législative devrait établir un comité spécial qui lui signalera dans les douze mois suivants les résultats de son examen et les amendements qu'il propose.

On s'est inquiété que le gouvernement ne modifie la loi avant que le comité n'ait achevé ses travaux. Il semble maintenant que le gouvernement permettra au comité d'entendre des témoignages que la loi ne soit modifiée.

L'Alberta a déposé le projet de loi n° 1, qui vise à étendre les dispositions de la loi *Freedom of Information and Protection of Privacy Act* aux écoles, aux pouvoirs sanitaires, aux institutions postsecondaires et aux municipalités, et qui assujettirait les organismes publics locaux aux dispositions de la loi, secteur par secteur, à mesure qu'ils sont prêts. On s'attend à ce que le secteur de l'éducation soit le premier nouveau groupe auquel la loi s'appliquera, suivi des secteurs de la santé et des municipalités.

Le gouvernement a aussi publié un document de travail intitulé *Striking the Right Balance* dans le cadre de l'élaboration de la nouvelle loi sur les soins de santé. Le point crucial est d'établir un équilibre entre le partage de l'information en vue d'améliorer la santé et les soins de santé et le besoin de protéger les renseignements médicaux des particuliers. Les résultats des consultations permettront d'élaborer un projet de loi qui sera déposé plus tard en 1997.

Le Manitoba prévoit de déposer un nouveau projet de loi sur la liberté d'information et la protection de la vie privée, qui viendra remplacer la Loi sur la liberté d'accès à l'information de 1988, qui porte seulement sur l'accès aux documents personnels. La nouvelle loi comprendrait un code d'accès équitable à l'information, qui régirait la collecte, l'utilisation et la communication, par le gouvernement, des renseignements personnels des résidents. Elle traiterait aussi de l'impact de l'application croissante de la technologie de l'information sur les droits à l'information.

En outre, la province envisage d'adopter une loi distincte sur la protection des renseignements médicaux pour renforcer les dispositions sur la confidentialité des renseignements touchant à la santé qui figurent dans nombre de différentes lois, et répondre aux préoccupations croissantes au sujet de la protection des

Les conférences annuelles se tiennent dans plusieurs buts, dont le plus important est l'échange de vues sur les questions de vie privée, qui sont de plus en plus sans frontières. Le Canada peut apprendre beaucoup en étudiant les initiatives d'autres pays en matière de protection des renseignements personnels, et nos propres organismes de vie privée ont beaucoup à offrir aux autres administrations. Dans un contexte où les ressources publiques, qui se font de plus en plus rares, sont réorientées vers des programmes et des systèmes qui menacent la vie privée, il y a peu de ressources disponibles pour sa protection. La conférence des commissaires à la protection des données offre la possibilité d'une certaine synergie.

Nombre des exposés sont disponibles sur notre site web Internet, au <http://infoweb.magi.com/~privcan/>. Le Commissariat dispose aussi d'un nombre limité de copies papier.

Conférence internationale des commissaires à la vie privée à Ottawa

En septembre dernier, le Commissariat a parrainé la 18^e Conférence internationale des commissaires à la vie privée et à la protection des données, qui s'est tenue à Ottawa. La conférence, qui était à l'origine une rencontre annuelle informelle des commissaires à la vie privée et à la protection des données de l'Europe de l'Ouest, est devenue un événement où échanger des renseignements et étudier les incidences sur la vie privée des nouvelles tendances et technologies.

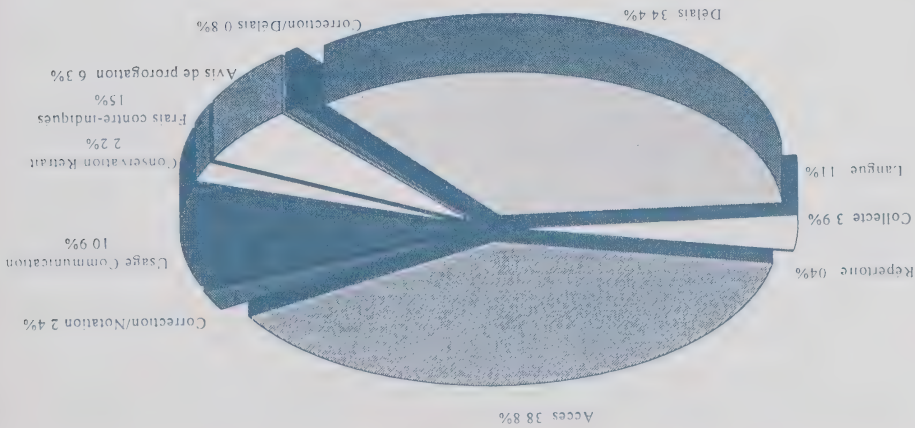
La conférence de 1996 a attiré 300 commissaires provinciaux, territoriaux et étrangers; pour la première fois, nombre de représentants de l'industrie et de défenseurs de la vie privée de partout dans le monde y participaient. Les commissaires venaient de 23 pays et 17 administrations internationales (par exemple, les provinces du Canada et les États d'Allemagne).

La conférence, dont le thème était *La vie privée et les données nominatives*, était axée sur l'impact que le commerce international en expansion a sur les renseignements personnels. Elle a attiré, pour la première fois, un nombre important de participants de l'Amérique du Nord, ainsi que des participants d'autres pays qui s'intéressent à la démarche adoptée en Amérique du Nord en matière de protection des renseignements personnels.

Les deux premiers jours, qui comportaient des exposés et des débats de spécialistes, étaient ouverts à tous les participants. Lors de la dernière journée, les commissaires à la vie privée et leur personnel ont procédé à une échange de vues sur les questions d'ordre administratif, juridique et de politique communes à leurs activités. On trouvait au nombre des sujets débattus lors des séances publiques :

- la nouvelle directive de l'Union européenne sur la protection des données et de la vie privée, et son impact sur les entreprises de l'Amérique du Nord;
- la surveillance accrue des particuliers, y compris la surveillance en milieu de travail et l'utilisation des renseignements sur les allées et venues d'une personne;
- les développements internationaux en matière de lois sur la protection des données et la vie privée;
- la protection des renseignements personnels et des industries choisies du secteur privé canadien.

Plaintes réglées par motifs



Origine des plaintes réglées

Origine	Nombre	TOTAL
Terre-Neuve	13	2,717
Île-du-Prince-Édouard	4	
Nouvelle Écosse	60	
Nouveau Brunswick	68	
Québec	644	
Région de la capitale nationale - Québec	36	
Région de la capitale nationale - Ontario	506	
Ontario	646	
Manitoba	54	
Saskatchewan	88	
Alberta	186	
Columbia Britannique	395	
Yukon	5	
Territoires du Nord-Ouest	1	
Hors Canada	11	

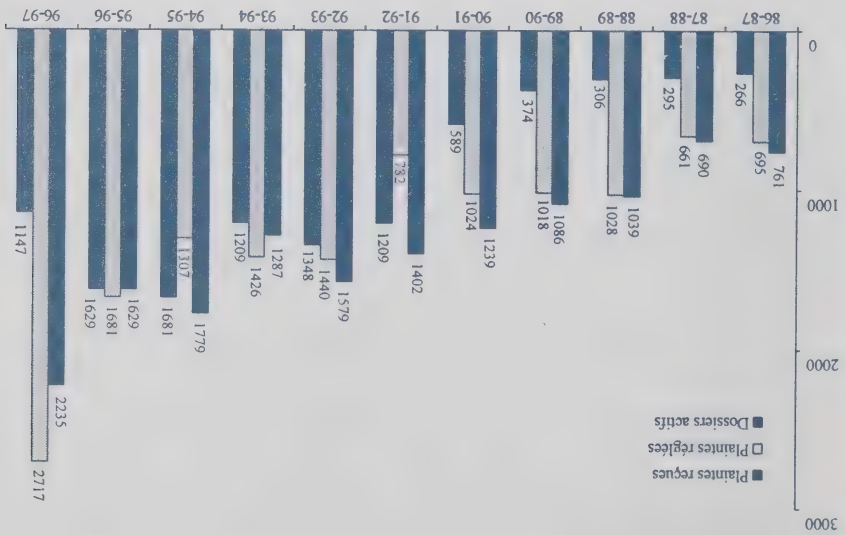
Plaintes réglées par institutions et résultats

Institution		Total	Fondée	Fondée; résolue	Non fondée	Abandonnée	Résolue	Réglées
Conseil du Trésor du Canada, Secrétaire	6	0	1	3	0	0	0	2
Conseil national de recherches Canada	1	0	0	1	0	0	0	0
Défense nationale	429	187	10	79	90	1	62	
Développement des ressources humaines Canada	176	35	24	45	25	8	39	
Diversification de l'économie de l'Ouest Canada	1	0	0	0	0	0	1	
Environnement Canada	19	0	9	8	0	0	2	
Gendarmerie royale du Canada	162	3	4	103	10	7	35	
Industrie Canada	12	0	0	5	3	0	4	
Justice, Ministère de la	209	2	1	20	179	5	2	
Monnaie royale canadienne	1	0	1	0	0	0	0	
Patrimoine canadien	8	0	1	1	5	1	0	
Pêches et Océans	11	1	1	1	0	0	8	
Ponts Jacques-Cartier et Champlain Inc.	4	0	3	0	0	0	1	
Ressources naturelles Canada	4	0	2	1	0	1	0	
Revenu Canada - Impôt, douanes et accise	231	100	7	74	17	7	26	
Santé Canada	17	7	0	3	1	3	3	
Service canadien du renseignement de sécurité	73	0	3	52	4	1	13	
Service correctionnel Canada	731	293	24	269	50	19	76	
Société canadienne d'hypothèques et de logement	5	1	0	1	2	0	1	
Société canadienne des Ports	1	0	0	1	0	0	0	
Société canadienne des Postes	112	5	5	71	9	10	12	
Société du crédit agricole Canada	6	0	2	2	0	0	2	
Solliciteur général Canada	2	0	0	0	0	0	2	
Statistiques Canada	3	1	0	1	0	0	1	
Transports Canada	31	9	2	7	4	1	8	
Travaux publics et Services gouvern. Canada	11	1	0	6	2	0	2	
TOTAL	2,717	770	116	925	468	81	357	

Plaintes réglées par institutions et résultats

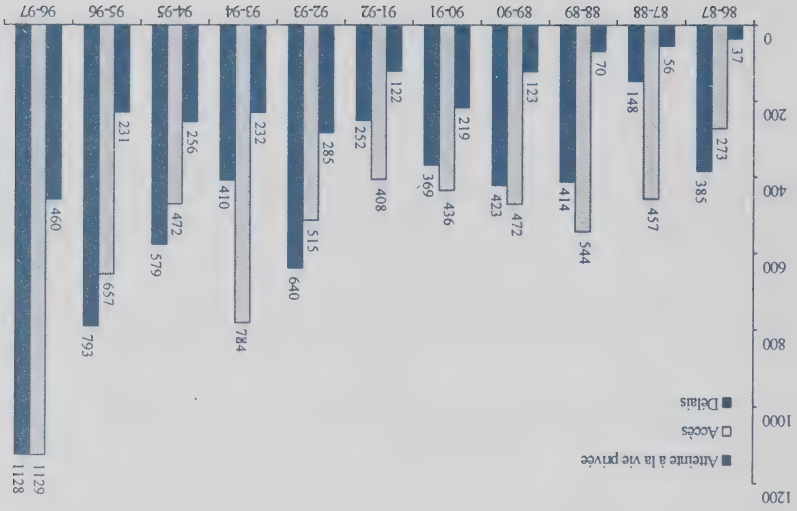
Institution		Total	Fondée	Fondée; résolue	Non fondée	Aban- donnée	Résolue	Régles
Affaires étrangères et Commerce int. Canada	10	6	0	4	0	0	0	0
Affaires indiennes et du Nord Canada	22	1	1	13	6	0	0	1
Agence canadienne de développement int.	1	0	0	0	0	1	0	0
Agence canadienne d'évaluation environnementale	1	0	0	1	0	0	0	0
Agence spatiale canadienne	22	0	0	18	0	4	0	0
Agriculture et Agro-alimentaire Canada	16	1	0	2	10	1	2	0
Anciens combattants Canada	4	0	0	3	0	1	0	0
Archives Nationales du Canada	55	9	0	29	6	0	11	0
Banque du Canada	1	0	0	1	0	0	0	0
Banque fédérale de développement	5	4	0	0	0	0	1	0
Bibliothèque nationale du Canada	1	0	0	0	1	0	0	0
Bureau du Conseil Privé	5	1	0	3	0	1	0	0
Bureau du vérificateur général du Canada	2	0	0	0	2	0	0	0
Centre national des Arts	1	0	0	0	0	0	1	0
Citoyenneté et immigration Canada	122	39	8	37	11	4	23	0
Commission canadienne des droits de la personne	18	1	3	11	0	1	2	0
Com. de l'immigration et du statut du réfugié	93	54	1	15	21	0	2	0
Commission de la fonction publique du Canada	24	5	1	13	3	1	1	0
Com. des plaintes du public contre la GRC	15	0	0	5	0	1	9	0
Commission nat. des libérations conditionnelles	27	4	2	11	7	2	1	0
Conseil de la radiodiffusion et des télécommunications canadiennes	3	0	0	3	0	0	0	0
Conseil de recherches en sciences humaines	1	0	0	0	0	0	1	0
Conseil de recherches en sciences naturelles et en génie	1	0	0	1	0	0	0	0
Conseil des arts du Canada	1	0	0	1	0	0	0	0

Plaintes 1986-97



* Le tableau reflète des variances minimales apportées aux statistiques pour les années 1993-94 à 1995-96

Plaintes réglées et motifs 1986-97

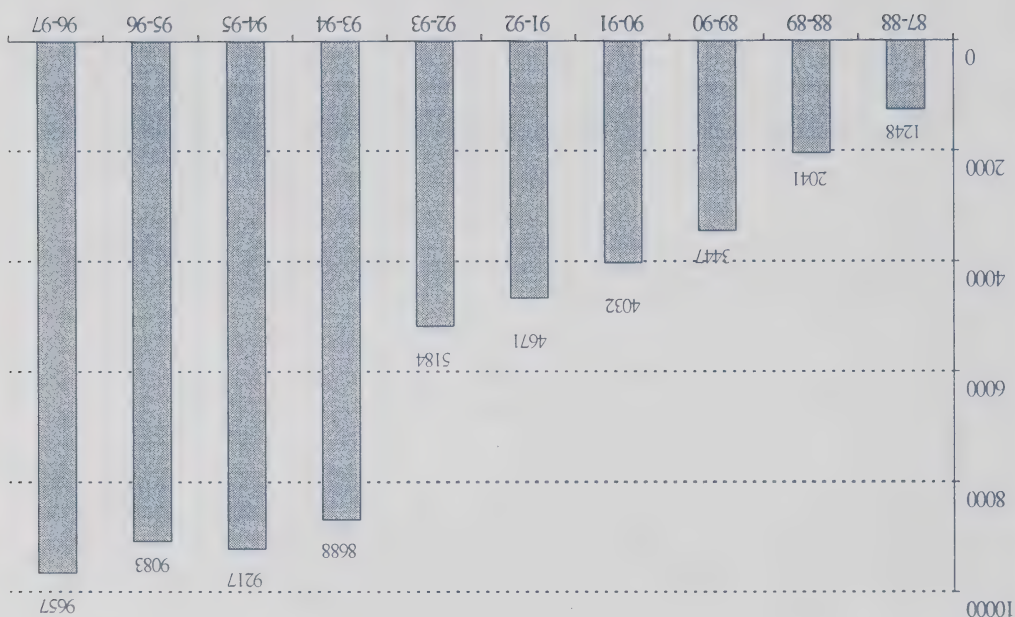


Les dix ministères les plus visés selon les plaintes reçues

Motifs					
Ministère		TOTAL	Accès	Délais	Vie privée
Service correctionnel Canada		602	134	422	46
Défense nationale		389	93	267	29
Revenu Canada		215	70	89	56
Justice, Ministère de la		208	101	97	10
Développement des ressources humaines		141	53	38	50
Com. de l'immigration et du statut du réfugié		115	65	38	12
Citoyenneté et immigration Canada		110	66	38	6
Gendarmerie royale du Canada		86	57	2	27
Société canadienne des Postes		69	37	7	25
Service canadien du renseignement de sécurité		45	44	1	0
AUTRE		255	108	66	81
TOTAL		2,235	828	1,065	342

Plaintes réglées par motifs et résultats

Résultats											
Motifs		Fondée	Fondée; résolue	Non fondée	Aban- donnée	Résolue	Réglée	TOTAL	Accès		
		20	77	468	234	69	261	1,129			
		Accès	20	76	443	227	62	227			
		Correction/Annotation		0	0	25	5	4			
		Frais contre-indiqués	0	1	0	2	0	1			
		Répertoire	0	0	0	0	1	0			
		Langue	0	0	0	0	2	1			
Atteinte à la vie privée		46	39	183	98	11	83	460			
		Collecte	3	0	54	19	4	25			
		Conservation/Retrait	11	12	20	8	2	6			
		Usage/Communication	32	27	109	71	5	52			
Délais		704	0	274	136	1	13	1,128			
		Correction/Délais	7	0	5	4	1	6			
		Délais	690	0	109	129	0	7			
		Avis de prorogation	7	0	160	3	0	0			
TOTAL		770	116	925	468	81	357	2,717			



Demandes de renseignements 1987-97

Erreurs sur des dossiers de crédit

Nous continuons de recevoir nombre d'appels de personnes inquiètes parce que des erreurs se sont glissées dans leur dossier de crédit. Les bureaux de crédit du Canada sont des entreprises privées et ne sont donc pas assujettis aux dispositions de la *Loi sur la protection des renseignements personnels*. Ils sont régis par les lois provinciales de protection des consommateurs de sorte que les détails des droits et responsabilités des parties varient de province en province. Les personnes qui n'ont pu obtenir la correction des erreurs par les bureaux de crédit locaux devraient contacter les organismes qui administrent la loi sur la protection du consommateur dans leur province.

protégée par les dispositions de la *Loi sur la protection des renseignements personnels* et de la *Loi sur les élections*, et que les électeurs qui n'y sont pas inscrits ont quand même le droit de voter. Les électeurs ont aussi le droit de faire retirer leurs noms de la liste ou de le transférer à leurs provinces ou territoires en écrivant au Directeur des élections.

sur des questions comme le télémarketing et le publipostage direct, l'adoption, la génétique, l'évaluation de crédit, les institutions financières et les dossiers médicaux.

Hydro-Québec demande aux nouveaux clients leur NAS

Nombre de Canadiens considèrent que le gouvernement fédéral ait le gardien et le surveillant du numéro d'assurance sociale, et que le Commissaire à la vie privée en est le gardien national. En réalité, il n'en est rien. Le gouvernement fédéral limite de façon stricte les utilisations qu'il fait du NAS, mais il n'a pas le pouvoir d'en contrôler les utilisations externes. On peut illustrer la situation par le fait suivant. Lorsque Hydro-Québec a demandé à ses nouveaux clients leur NAS, le Commissaire fédéral a reçu un nombre astronomique d'appels lui demandant d'intervenir parce qu'il s'agit d'un numéro fédéral.

Le Commissaire à l'information et à la vie privée du Québec et Hydro-Québec (qui est assujettie à la loi provinciale sur la protection des renseignements

personnels) ont débattu la question et semblent se diriger vers les tribunaux. Par consentement mutuel, les deux parties ont accepté de reculer et de trouver un compromis. Hydro-Québec a convaincu le commissaire provincial que le recours au NAS est le seul moyen de retracer les clients qui démenagent sans régler leur compte. À son tour, le commissaire a amené Hydro-Québec à créer un nouveau numéro d'identification unique, à éliminer certains détails injustifiés de ses dossiers et à permettre à son personnel de recouvrer seulement d'avoir accès au NAS. En mai 1996, l'Assemblée nationale du Québec a adopté l'article 8 du décret 634 d'Hydro-Québec qui donne à la compagnie le droit de demander aux clients « ouvrant un compte » leur NAS. Lorsque Hydro-Québec a commencé à faire savoir qu'elle demanderait à ses clients leur NAS, les téléphones ont commencé à sonner.

Le commissaire fédéral à la vie privée continue de s'opposer à ce que l'on force les gens à fournir leur NAS pour des utilisations tout à fait sans lien avec l'utilisation première. Toutefois, étant donné que les décrets d'Hydro-Québec exigent maintenant le NAS, ses clients n'ont pas le droit légalement de refuser.

Nouvelle liste électorale permanente

Le Commissariat a reçu plusieurs appels de personnes qui étaient troublées parce que Elections Canada leur demandait leur date de naissance sur le formulaire de recensement pour la nouvelle liste électorale permanente (voir la page 23 pour obtenir plus de détails). Elections Canada demande la date de naissance et le sexe pour pouvoir distinguer entre des personnes de noms identiques ou semblables. Cette information ne figure pas sur les listes fournies aux parties politiques chaque année. Les agents expliquent que la liste électorale permanente est

avait été accordé), que l'Archiviste ne pouvait faire enquête sans collaboration du MDN et que ce ministère ne pouvait mener d'enquête sans connaître les allégations portées contre lui.

Ayant conclu que l'auteur souhaitait clairement la tenue d'une enquête, l'Archiviste a donc achevé les renseignements dans ce but. Comme les Archives ne sont pas autorisées à faire enquête, il était raisonnable qu'elles acheminent les allégations au MDN. En fait, les Archives ont utilisé les renseignements dans le but pour lequel ils avaient été fournis.

Un des principes fondamentaux de la justice naturelle est qu'un accusé a le droit de faire face à son accusateur et de connaître les accusations portées contre lui. Cela s'applique même aux plaintes déposées aux termes de la *Loi sur la protection des renseignements personnels* : le nom et les accusations du plaignant sont transmis au ministère visé. Le Commissaire a jugé que la plainte n'était pas fondée.

Demandes de renseignements

Le Commissariat a reçu plus de 9 600 demandes de renseignements cette année. Ces demandes vont de questions simples au sujet de la *Loi sur la protection des renseignements personnels* à la façon d'obtenir une réhabilitation, le retrait de noms sur les listes de publicité postale, ou la façon de retracer des parents. Chaque fois que le gouvernement fédéral lance un nouveau programme ou entreprend de recueillir des renseignements personnels (dernier recensement, étude sur l'indice des prix à la consommation, couplage des données de Douanes et de l'assurance-emploi, etc.), les téléphones se mettent à sonner.

Une partie importante du travail consiste à orienter les personnes vers les organismes qui peuvent le mieux les aider. Il est manifeste qu'un certain nombre de personnes sont agacées lorsqu'elles découvrent les limites du mandat du Commissariat et sont en colère lorsqu'il n'existe aucune disposition juridique pour la protection de leur vie privée. Nous les incitons à appuyer l'initiative du gouvernement d'adopter d'ici à l'an 2 000 une loi nationale sur la protection de la vie privée.

Environ 40 p. 100 des demandes de renseignements relèvent de la compétence du Commissaire et portent sur l'utilisation et l'interprétation de la *Loi sur la protection des renseignements personnels*. Le groupe de renseignements suivant, soit les demandes de publications et les appels des médias, totalisent 18 p. 100 des appels. Les renvois à nos homologues provinciaux comptent pour 8 p. 100, et les plaintes au sujet des utilisations du numéro d'assurance sociale, pour 7 p. 100 (voir ci-dessous). Le reste des demandes de renseignements, soit 27 p. 100, portent

Une formatrice fait circuler les renseignements des étudiants Une étudiante suivant un cours à un centre de formation privé dont les services avaient été retenus par contrat par Ressources humaines Canada (RHC) s'est plainte que la formatrice avait fait circuler une liste renfermant les nom, adresse, numéro de téléphone et numéro d'assurance sociale des étudiants pour que chaque étudiant vérifie ses renseignements. Par la même, elle communiquait effectivement des renseignements personnels à chaque étudiant. L'étudiante était d'avis que le centre de formation devait payer une amende.

Il n'y a pas de doute que le centre de formation privé avait un contrat avec RHC et que, par conséquent, il était tenu de respecter la *Loi sur la protection des renseignements personnels*. En outre, il est certain qu'il y a eu communication de renseignements personnels. L'enquêteur a interviewé la formatrice; cette dernière a confirmé que RHC lui avait signalé qu'elle était chargée de veiller à la protection des renseignements personnels de ses étudiants. Elle a aussi confirmé que le centre utiliserait désormais des feuilles individuelles.

L'enquêteur a expliqué à la plaignante qu'aucune amende ne serait imposée au centre de formation, car c'est RHC qui est tenu responsable des actions de ses entrepreneurs. La plainte a été jugée fondée.

Une demande d'enquête aux Archives ne constitue pas un renseignement personnel Une lettre demandant à l'Archiviste national d'enquêter sur des allégations de destruction incorrecte de documents au ministère de la Défense nationale (MDN) a suscité une plainte de la part de l'auteur à l'effet que la lettre n'aurait pas dû être communiquée au MDN.

La lettre précisait les allégations de l'auteur, identifiait des sources au MDN susceptibles de fournir de l'information et demandait à l'Archiviste de faire enquête. Comme les Archives nationales n'ont pas le droit de se rendre dans un ministère pour enquêter de leur propre chef, l'Archiviste a transmis une copie de la lettre au sous-ministre de la Défense nationale en lui demandant de faire enquête.

Le plaignant a soutenu que la lettre contenait des renseignements personnels et confidentiels, comme le nom de ses sources, qui n'auraient pas dû être divulgués et que la communication par les Archives de sa lettre au MDN enfreignait sa vie privée.

Les Archives ont soutenu que la lettre portait un en-tête commercial et qu'elle ne paraissait donc pas constituer une lettre personnelle, que l'auteur ne demandait pas la confidentialité (ce qu'il avait demandé dans une lettre antérieure, et qui lui

L'inspecteur relève de nombreuses lacunes qu'il émet une lettre de constatations distincte. La lettre de l'inspectrice faisait état d'infractions spécifiques et de son interprétation des remarques du directeur de bord à l'effet que la compagnie devrait être blâmée pour les lacunes relevées, et non lui, puisque l'équipage se plaignait depuis un certain temps du fait que les considérations en matière de service l'emportait sur celles au titre de la sécurité. Le directeur de bord a affirmé que ses remarques avaient été mal interprétées.

Les inspecteurs de la compagnie aérienne jugent que les entrevues avec les équipages sont une source importante de renseignements puisque les équipages leur confient souvent des préoccupations qu'ils hésiteraient à signaler à leur employeur. Une bonne communication entre les inspecteurs et les équipages est essentielle. Toutefois, la sécurité demeure la considération primordiale. Lorsqu'un inspecteur juge que l'équipage ne respecte pas les consignes de sécurité, il doit le signaler à la direction de la compagnie aérienne. Cette dernière, à son tour, doit signaler par écrit à Transports Canada les mesures correctives prises. De même, le directeur de bord a l'entière responsabilité du service, de la sécurité et du personnel de bord et il peut faire l'objet de mesures disciplinaires en cas d'infractions majeures. Ce sont les compagnies aériennes qui déterminent habituellement les mesures disciplinaires qui s'imposent, mais Transports Canada peut émettre des suggestions et des recommandations précises.

La loi, les règlements et les manuels de procédures autorisent Transports Canada à mener des inspections de la sécurité aérienne et à communiquer ses constatations, y compris les observations des équipages, aux compagnies aériennes. L'inspectrice a jugé que les remarques de l'équipage étaient pertinentes à la sécurité aérienne et elle a demandé à la compagnie aérienne de prendre les mesures correctives nécessaires. Le Commissaire a conclu que Transports Canada est clairement autorisé par la loi à mener des inspections de la sécurité et que l'inspectrice a communiqué les remarques de l'équipage aux fins pour lesquelles elle les avait recueillies, soit la correction des lacunes relevées. En conclusion, la Loi sur la protection des renseignements personnels n'a pas été enfreinte.

Néanmoins, le Commissaire a reconnu que le fait de paraphraser les remarques d'un équipage peut être cause de mauvaise interprétation, en particulier si l'équipage ne voit pas le rapport écrit et n'a pas la possibilité de rectifier les malentendus. Les remarques sont souvent recueillies lorsque l'équipage est occupé lors de l'atterrissage, qui peut susciter des observations qui ne sont pas toujours prudentes. Le Commissaire a recommandé que les inspecteurs communiquent leurs constatations aux équipages avant de les soumettre à la compagnie aérienne. Il a aussi recommandé qu'ils s'efforcent davantage, pour éviter une interprétation incorrecte, de noter *verbatim* les remarques de l'équipage.

pertinents pour assurer que les indemnités de démenagement étaient déclarées de façon adéquate.

Revenu Canada a revu le ruban informatique et étudié les déclarations de tous les membres à qui une indemnité avait été versée au cours des trois années visées. Sur un total de 1 400 déclarations d'impôt, 633 ont été réévaluées et 1 227 000 dollars en impôts non payés ont été recouvrés. Le reste des déclarations a été traité sans qu'un changement ne soit apporté, soit parce que le membre ne s'était pas prévalu de l'indemnité, soit parce que la déclaration avait déjà été réévaluée par le bureau régional au cours du processus de révision postérieures.

Le Commissaire était clairement d'avis que les deux ministères étaient au fait des restrictions contenues dans la *Loi sur la protection de la vie privée* et la *Loi sur l'impôt sur le revenu*, avaient obtenu l'avis de leur avocats et avaient agi avec prudence. La GRC est tenue de signaler de façon appropriée à Revenu Canada toutes les indemnités qu'elle verse à ses employés. Plutôt que de demander à la GRC d'émettre une nouvelle série de T4 à tous ses membres pour les années visées (ce qui aurait déclenché une révision de tous les dossiers des membres), Revenu Canada a fait porter sa demande sur les membres qui avaient obtenu une indemnité de démenagement. Le Commissaire a conclu que Revenu Canada était autorisé à recueillir les renseignements aux termes de la *Loi sur l'impôt* et que, par conséquent, la *Loi sur la protection des renseignements personnels* n'avait pas été enfreinte.

Une inspectrice de la sécurité communique les remarques d'un équipage à la compagnie aérienne. La communication à un employeur des critiques faites par un employé peut avoir un effet prévisible et exige qu'on évalue soigneusement si les remarques constituent simplement du dédoublement ou de l'information à laquelle l'employeur a droit. Cette situation est bien illustrée par le cas suivant : un directeur de bord d'Air Canada aurait dit à une inspectrice de Transports Canada que nombre de lacunes notées lors d'un vol transatlantique résultaient de l'accent mis par la compagnie aérienne sur le service au détriment de la sécurité. L'inspectrice a paraphrasé toutes les remarques des membres d'équipage et les a transmises à la compagnie aérienne dans son rapport. À la lumière du rapport, cette dernière a corrigé les lacunes relevées et soumis le directeur de bord à des mesures disciplinaires. Ce dernier s'est plaint par la suite que la communication par l'inspectrice de ses propos était incorrecte.

L'enquêteur a établi que l'inspectrice avait noté de nombreuses infractions à la *Loi sur l'aéronautique*, au Règlement de l'air et aux ordonnances sur la navigation aérienne. Normalement, le rapport d'inspection est acheminé tous les mois au personnel pertinent de la compagnie aérienne. C'est seulement lorsque

Le Commissaire partageait l'avis de la plaignante à l'effet que l'accès devrait toujours être contrôlé et autorisé par le superviseur de l'employé. Suite à la plainte, le personnel informatique doit maintenant obtenir la permission écrite du superviseur avant de modifier un mot de passe.

Les gestionnaires et les employés doivent se rappeler que le courrier électronique n'est pas protégé et que même les messages électroniques effacés peuvent parfois être récupérés. En bref, les systèmes informatiques ne devraient pas servir à mémoriser ou à achever des renseignements qu'on ne veut pas que d'autres consultent. La plainte a été jugée non fondée.

Révision des cotisations d'impôt pour les indemnités de déménagement : pas de consultation à l'aveuglette. Plusieurs membres de la GRC ont porté plainte auprès du Commissaire à l'effet qu'en fournissant à Revenu Canada une liste des membres ayant reçu des indemnités de déménagement entre 1991 et 1993, la GRC avait communiqué de façon inappropriée leurs renseignements personnels. (Ils se sont aussi plaint de la collecte des renseignements par Revenu Canada). Selon les plaignants, la demande constituait un moyen aveugle d'obtenir des renseignements; Revenu Canada était tenu, aux termes de la *Loi de l'impôt sur le revenu*, d'obtenir un ordre de la cour pour obtenir des renseignements sur des personnes non désignées par leur nom et que, par conséquent, la GRC n'aurait pas dû soumettre la liste sans en avoir l'ordre de la cour.

La question concernait l'indemnité versée aux membres de la GRC lors d'un déménagement. Cette indemnité, qui équivaut à un douzième du salaire annuel, est imposable à la source par la GRC et doit être signalée par un membre sur sa déclaration d'impôt de l'année en cours comme bénéfice imposable. Les membres sont avisés de ce fait lors du versement de l'indemnité. Par contre, les frais de déménagement réels, avec recus à l'appui, sont pleinement déductibles.

Une vérification faite par Revenu Canada auprès des membres de la GRC du district de Regina a révélé que nombre de membres déduisaient simplement le plein montant de l'indemnité à titre de frais de déménagement. Les vérificateurs ont également découvert que la GRC n'avait pas bien inscrit l'indemnité imposable sur les formulaires T4 des membres. Autrement, Revenu Canada aurait découvert que les renseignements ne correspondaient pas aux données conservées dans son propre ordinateur et n'aurait pas eu besoin de la liste de la GRC. Lorsqu'il a repéré cette omission, Revenu Canada a demandé à la GRC les listes afin de déterminer par échantillonnage aléatoire l'étendue du problème. Suite à une conversation téléphonique entre le Commissaire de la GRC et le sous-ministre de Revenu Canada, la GRC a consenti à achever les dossiers

secteur privé la demande; cette pratique ne relève pas de la compétence du gouvernement fédéral. Le Commissaire a rejeté la plainte.

Les employés doivent-ils s'attendre à ce que leurs messages électroniques soient protégés ? Selon une employée du Centre de traitement des Services correctionnels du Canada (SCC), la secrétaire de division aurait obtenu en son absence son mot de passe et l'accès à son courrier électronique sans son consentement. Elle s'est plainte que cela contrevient à la protection de ses renseignements personnels et des renseignements, appartenant aux détenus, qui étaient conservés dans sa base de données.

L'enquêteur a établi que l'administration centrale de SCC avait demandé une copie d'un document que la plaignante avait préparé, mais ne l'avait pas reçu. En raison de l'urgence de la demande et en l'absence de la plaignante, la secrétaire de cette dernière, qui savait que le document avait été envoyé et pouvait être trouvé dans le courrier électronique de la plaignante, a donc demandé l'aide de la secrétaire de la division. Le personnel informatique a suggéré de modifier le code d'accès pour permettre à la secrétaire d'obtenir le document. Le directeur adjoint de l'établissement de détention a autorisé la secrétaire à modifier le code d'accès au courrier électronique.

La plaignante a soutenu qu'une copie aurait pu être obtenue d'un autre bureau. Elle soupçonnait son superviseur de vouloir prendre connaissance de ses échanges électroniques avec un représentant syndical et un autre employé dans le cadre d'une plainte de harcèlement déposée contre lui. En fait, seule la secrétaire a eu accès à l'ordinateur de la plaignante et elle a soutenu qu'elle n'avait pas parcouru les messages électroniques ou les dossiers personnels. Comme elle connaissait la date approximative d'achèvement du message, elle avait été en mesure de retracer rapidement le document pertinent.

L'enquêteur n'a pas trouvé de preuves indiquant qu'il y avait eu communication non autorisée de renseignements personnels. Dans le cas d'un ordinateur, un mot de passe équivalant à un cadenas et à une liste d'accès pour un document papier. Le mot de code vise à empêcher l'accès non autorisé par une personne qui n'a pas besoin de consulter les renseignements contenus dans les dossiers de travail d'un employé. Toutefois, indépendamment du support de l'information, les renseignements qu'un employé prépare dans le cadre de la poursuite des affaires du gouvernement et stocke dans les locaux du gouvernement devraient être accessibles au superviseur de l'employé s'il y a un besoin réel de consulter ces renseignements en l'absence de l'employé.

jours, s'il existe des raisons valables de conserver un dossier pendant plus que 90 jours. Le Commissaire a conclu que la plainte déposée contre les Archives était fondée, mais la mise en oeuvre du système de rappel des dossiers a clos le cas. Il a rejeté la plainte déposée contre le ministère des Anciens Combattants.

À l'origine d'une plainte : les renseignements fournis par un plaignant

Il arrive très souvent qu'une personne ne saisisse pas bien les incidences d'un emprunt d'argent, et de la collecte et la divulgation de renseignements personnels qui font partie intégrante du processus de demande de prêt. Un homme s'est plaint d'avoir reçu d'un cabinet d'avocats, au sujet de son prêt d'études du Canada, une lettre qui renfermait des renseignements au sujet de sa déficience cardiaque et portait son numéro d'assurance sociale. Il voulait savoir comment ces renseignements avaient été obtenus.

Comme l'homme n'avait pas payé son prêt, RHC avait remis le recouvrement entre les mains d'une agence, soit le cabinet d'avocats. Ce dernier a obtenu une évaluation de crédit de l'agence Equifax (qui est un bureau de crédit important) qui renfermait des renseignements médicaux concernant le plaignant, le nom de son médecin et une note à l'effet que ces renseignements avaient été fournis par le plaignant lui-même au cours d'une entrevue.

Un prêt étudiant est comme un prêt commercial. L'étudiant emprunte l'argent d'une institution financière et autorise le prêteur à échanger de l'information avec les bureaux de crédit, les octroyeurs de crédit et les agences d'évaluation de crédit au sujet du prêt. Cela fait partie de l'entente entre l'emprunteur et le prêteur. Le programme de prêts aux étudiants sert de garantie à la banque. Si l'étudiant ne rembourse pas son prêt, la banque obtient le paiement du prêt par le gouvernement, qui tente à son tour de recouvrer la somme due.

Le cabinet d'avocats agissait à titre de mandataire du ministère dans sa tentative pour recouvrer le prêt et avait une raison légitime d'obtenir un rapport de crédit d'Equifax. En fait, il a agi dans l'intérêt du plaignant lorsqu'il lui a expliqué que RHC pourrait retarder son recouvrement si le plaignant pouvait fournir des renseignements confirmant que son handicap l'empêchait de travailler et de payer son prêt.

Le ministère a aussi établi que le programme de prêts pour étudiants du Canada est un programme fédéral autorisé à utiliser le numéro d'assurance sociale (NAS) et que le cabinet d'avocats, à titre de mandataire, avait aussi le droit de l'utiliser; de plus, le NAS figurait dans le dossier qu'Equifax détenait sur le prêteur. Les agences de crédit utilisent le NAS et c'est la raison primordiale pour laquelle le

conservent tous les vieux dossiers des employés gouvernementaux et des militaires) et le ministère des Anciens Combattants n'ont pu parvenir à retracer son dossier, l'ancien combattant a porté plainte auprès du Commissariat. La demande originale de l'ancien combattant avait été présentée au ministère des Anciens Combattants. Toutefois, parce que le dossier datait de plus de deux ans, elle avait été acheminée aux Archives nationales, qui ont découvert que le dossier manquait, mais qui avaient néanmoins en mains un formulaire indiquant que le dossier avait été acheminé en 1987 au ministère des Anciens Combattants. À part la conservation de ce formulaire, les Archives nationales ne disposaient d'aucun mécanisme de suivi pour assurer le retour du dossier.

Le ministère des Anciens Combattants photocopie habituellement l'original à Ottawa, l'achemine aux Archives et en fait parvenir des copies aux bureaux régionaux pertinents. Il n'a pas réussi à retracer le dossier et était d'avis qu'il avait été retourné aux Archives. Un système informatique permet maintenant de suivre les dossiers prêts et d'assurer leur retour aux Archives, mais il n'a été mis en service qu'en 1991. Tous les dossiers papier antérieurs à 1987 auraient normalement été détruits dans le cadre du processus courant d'examen et de d'élimination des dossiers.

Lorsque le plaignant a produit une lettre provenant de la Légion royale canadienne déclarant que le personnel de la Légion avait revu son dossier en 1988 à l'appui de sa demande de pension, l'enquêteur a communiqué avec la Légion. Le personnel de la Légion était volontiers disposé à offrir son aide, mais il est vite devenu évident qu'il n'avait qu'étudié les originaux sur place, dans les bureaux du gouvernement, et photocopié les documents nécessaires sans emprunter les originaux. Heureusement pour le plaignant, ces copies ont été utiles. Par ailleurs, l'enquêteur a suivi sans succès une autre piste menant au bureau du Chef des services de santé du ministère de la Défense nationale.

L'enquêteur a dû conclure que le dossier était disparu ou avait été égaré dans l'énorme répertoire des Archives et que trop de temps s'était écoulé pour qu'on puisse espérer le retrouver. Si le système de contrôle des prêts des Archives avait été plus efficace, l'absence du dossier aurait été notée plus rapidement et les chances de le retracer auraient été bien meilleures. Le problème n'avait pas de solution immédiate, mais le Commissaire a demandé l'assurance qu'un tel incident ne se répéterait pas.

Suite à l'enquête, les Archives nationales ont mis sur pied un système de suivi et de rappel des dossiers prêts aux autres ministères. Les ministères recevront maintenant un rappel officiel après 90 jours; l'appel sera répété après 120 et 180

« questions d'emploi ». Surprise, elle a demandé comment l'entreprise avait obtenu les renseignements nécessaires pour entrer en contact avec elle et si l'entreprise était du secteur privé. L'entreprise a expliqué son statut et son rôle, mais la plaignante a été abasourdie par la communication de ses renseignements personnels à l'extérieur du ministère.

La Loi sur l'assurance-chômage autorise un ministère à communiquer des renseignements aux personnes lorsque le ministre le juge souhaitable. L'enquêteur a confirmé que le ministre en poste avait signé l'autorisation de communication de renseignements à des entrepreneurs aux fins précisées dans le contrat. Le ministère avait signé un contrat avec l'entreprise qui avait téléphoné à la plaignante pour lui signaler le cours.

Pour accroître la participation à la formation, le ministère avait communiqué les noms et numéros de téléphone de bénéficiaires cibles de l'assurance-chômage à l'entreprise de formation pour que cette dernière offre directement le cours aux bénéficiaires. Le ministère n'avait pas averti les bénéficiaires, ni demandé leur consentement, pour la communication des renseignements, et aucune mention n'en avait été faite dans la documentation à l'appui. Le cours n'était pas obligatoire, et sa tenue, qui visait à aider les bénéficiaires à mieux vivre les changements personnels suscités par la perte de l'emploi et les effets négatifs sur leur capacité à trouver un nouvel emploi, n'intéressait pas la dame. Puisque la formation n'était pas obligatoire et que le contrat n'autorisait pas la communication de renseignements personnels afin de promouvoir le cours, le Commissaire a jugé la plainte fondée. De plus, l'enquêteur a découvert que les contrats ne contenaient pas de clause protégeant les renseignements personnels qui étaient communiqués à l'entreprise.

À la suite de cette plainte, le Centre d'emploi du Canada consulte maintenant ses clients avant de communiquer leur nom aux entrepreneurs en formation. La description des renseignements recueillis et de leurs utilisations, selon ce qui figure dans *Info Source*, sera modifiée; le formulaire de demande de prestations d'assurance-chômage a été modifié et décrit maintenant les utilisations éventuelles des renseignements des clients en matière de formation. Enfin, les Centres d'emploi ont été avertis de veiller à ce que les contrats renferment une clause visant à protéger les renseignements personnels de leurs clients. En prenant en compte ces mesures, le Commissaire a estimé la plainte résolue.

Un nouveau système de suivi naît de la perte d'un dossier

En réclamant son dossier médical pour appuyer sa demande de pension d'invalidité, un ancien combattant de la Seconde Guerre mondiale a découvert que celui-ci avait apparemment été perdu. Lorsque les Archives nationales (qui

Alors qu'elle tentait de recueillir des preuves dans le cadre d'une enquête sur une fraude et un détournement de fonds fédéraux présumés, la GRC a écrit à neuf organismes pour obtenir une copie de tous les contrats signés avec la personne soupçonnée et le détail des versements qu'il lui avaient été faits. Les lettres contenaient de l'information au sujet de l'enquête; on y déclarait en particulier que les preuves obtenues jusqu'à présent étaient accablantes et qu'une poursuite était inévitable. La personne concernée a également porté plainte auprès de la Commission des plaintes du public contre la GRC.

La GRC doit être en mesure d'établir que la communication de renseignements personnels au cours d'une enquête est nécessaire à l'accomplissement de son mandat de maintien de l'ordre et d'enquête. Au cours de l'enquête menée par la Commission des plaintes du public contre la GRC, cette dernière a admis que la mention d'une poursuite n'était pas nécessaire et elle a offert ses excuses au plaignant pour tout inconvenient que cela aurait pu lui porter. Ainsi, de son propre aveu, la communication était excessive.

L'enquêteur à la protection des renseignements personnels a étudié les dossiers et trouvé l'original de la lettre, mais il n'a pu retracer d'énoncé identique, ou similaire, dans aucun des volumes précédents. Le commentaire paraît en premier lieu dans la lettre, et semble représenter l'avis de l'auteur. La GRC a reconnu que l'énoncé était inutile, abusif et dépourvu de tact. Le Commissaire de la GRC s'est engagé à veiller à ce que tous les policiers chargés de recueillir des preuves auprès d'organismes extérieurs dans le cadre des enquêtes sur les crimes économiques reçoivent une formation appropriée.

Le Commissaire à la protection de la vie privée a conclu que la plainte était fondée, mais il était au regret qu'on n'ait pu faire plus pour corriger la situation. RHC réserve ses communications aux entreprises de formation

Un des signes les plus tangibles et manifestes de la sous-traitance des services gouvernementaux concerne les cours de formation offerts aux bénéficiaires de l'assurance-chômage. Ces cours, qui étaient autrefois offerts par Ressources humaines Canada (RHC), sont maintenant confiés à des entreprises privées spécialisées en formation. Cela étonne souvent les bénéficiaires, qui se demandent comment ces entreprises ont obtenu leurs renseignements.

Prenons le cas de cette Albertaine qui avait quitté son emploi afin de suivre son conjoint inscrit à l'université d'une autre ville. Elle a présenté une demande à l'assurance-chômage deux semaines avant son déménagement en précisant sa nouvelle adresse. Peu après son déménagement, une entreprise l'a appelée pour lui offrir un cours de trois semaines, payé par le ministère, portant sur des

Communications de renseignements par la GRC jugée « excessive »
 Un avocat a contesté la communication par la GRC à plusieurs organismes de renseignements concernant son client, sur lequel portait une enquête. Il a soutenu que cette communication était excessive et enfreignait la *Loi sur la protection des renseignements personnels*.

Le Commissariat a offert ses conseils et son appui pour l'ébauche de mesures de contrôle appropriées, ce que le ministère a accepté. Il a hâte de connaître les résultats de l'exercice.

La question n'est pas de déterminer si un ministère peut imposer des mesures disciplinaires à ses employés en cas de conflits d'intérêt ou d'autres infractions, mais plutôt de veiller à ce que les dossiers de programme ne servent pas couramment à la supervision des employés. Les circonstances qui justifient l'utilisation des renseignements sans lien avec le travail devraient être graves, l'accès limité et l'autorisation d'accès bien précise.

consultation de la déclaration d'impôt d'un employé.

Revenu Canada sur des situations exceptionnelles semblables, notamment la renseignements personnels a suggéré à RHC de consulter les lignes directrices de d'une autre rencontre pour régler le différend, le personnel de la protection des l'assurance-chômage ne soient pas transmis à l'extérieur du ministère. À la suite qu'une disposition visant à s'assurer que les renseignements de l'Assurance-chômage sur lequel s'appuyait le ministère (article 96) était autre chose Le Commissaire a rejeté la proposition à l'effet que l'article de la *Loi sur*

protection des renseignements personnels autorise les utilisations conformes. de la collecte, soit l'administration de la *Loi sur l'assurance-chômage*. La *Loi sur la* Ses représentants ont aussi soutenu que l'utilisation était conforme au but original. professionnelisme et l'intégrité du personnel chargé d'administrer le programme. *Loi sur l'Assurance-chômage*, dont un élément essentiel est d'assurer le qu'il recueillait des renseignements afin d'administrer et de mettre en oeuvre la autorisait les communications stipulées dans certaines autres lois du Parlement et Le ministère a soutenu que la *Loi sur la protection des renseignements personnels*

La plaignante a soutenu que l'utilisation par RHC de son dossier de prestations aux fins d'emploi enfreignait la *Loi sur la protection des renseignements personnels* car cela équivalait à utiliser des renseignements recueillis à une fin—soit le paiement de ses prestations d'assurance-chômage—pour un usage sans aucun rapport avec le premier, soit la prise de mesures disciplinaires à son égard.

pressions des clients qui se plaignent fréquemment qu'ils ne reçoivent pas leur courrier à leur nouvelle adresse.

Toute personne qui prévoit de déménager et qui s'oppose à ce que sa nouvelle adresse soit communiquée aux entreprises de publicité postale en gros devrait lire le formulaire attentivement. Toute personne qui souhaite diminuer la quantité de publicité postale qu'elle reçoit peut aussi utiliser le service *Do Not Call/Do Not Mail* de l'Association canadienne de marketing direct à l'adresse suivante :

1 Concorde Gate, Suite 607
Don Mills, Ontario
M3C 3N6

Lignes directrices sur l'utilisation des dossiers du programme aux fins de supervision Certains gestionnaires cumulent deux fonctions dans leurs rapports avec leurs employés, car ils sont, d'une part, employeur et d'autre part, administrateur du programme. C'est un défi que d'établir la distinction entre ces deux rôles et de traiter de façon adéquate les employés. Par exemple, à la suite d'une plainte portée en 1993, Revenu Canada avait établi des lignes directrices sur l'utilisation des renseignements fournis par les contribuables à des fins de surveillance de son personnel ou pour la prise de mesures disciplinaires. Cette année, Ressources humaines Canada (RHC) a fait de même à la suite d'une plainte semblable.

La question qui se posait avait trait à l'enquête faite par l'employeur sur la demande de prestation d'assurance-chômage d'une femme. Les résultats de l'enquête ont servi à prendre des mesures disciplinaires contre cette femme, à titre d'employée. Celle-ci, une préposée à l'assurance auprès de l'ancien ministère de l'Emploi et de l'Immigration (maintenant Ressources humaines Canada (RHC)), avait connu de graves problèmes de santé et épuisé ses congés de maladie. Par la suite, elle avait demandé et reçu des prestations d'assurance-chômage.

Pour accélérer le paiement des prestations, elle avait livré en mains propres ses demandes, ainsi que celles de son fils, à ses collègues préposés à l'entrée manuelle des données dans le système. L'employée, surprise à le faire, avait été suspendue pendant huit jours et on l'avait avisée qu'elle était en conflit d'intérêt. Elle a néanmoins récidivé. Les gestionnaires du ministère se sont inquiétés des pressions que ce comportement exerçait en général sur ses collègues, surtout sur un collègue occupant un poste de confiance, et ils ont entrepris d'étudier son dossier d'assurance-chômage. L'employée a été remerciée de ses services après négociation d'un règlement hors cours.

Le fait d'assujettir les commissions aux dispositions de la Loi sur la protection des renseignements personnels n'entraverait pas leurs travaux, car la loi autorise la communication de renseignements personnels lorsque "des raisons d'intérêt public justifieraient nettement une éventuelle violation de la vie privée". Toutefois, ainsi assujetties, les commissions seraient tenues de déterminer soigneusement si une communication de renseignements sert clairement l'intérêt public, et devraient mettre sur pied un cadre visant l'accès, la communication et la conservation des documents d'enquête après l'achèvement de l'enquête.

Postes Canada énonce mieux son option de retrait sur l'avis de changement d'adresse Cette année, le Commissariat a achevé de longues négociations en vue de tenter de résoudre deux plaintes au sujet du service de changement d'adresse de Postes Canada.

Aux termes de ce service, le courrier des clients est réacheminé de l'ancienne adresse à la nouvelle lors de leur déménagement (contre frais). Parce qu'il fonctionne en mode de recouvrement des coûts, Postes Canada offre aussi un service de correction d'adresse aux entreprises de publicité postale en gros, commerciales et gouvernementales (aussi contre frais) et met à jour les adresses de leurs clients, sauf si le client s'y oppose activement.

Les plaignants s'opposaient à la mention, sur le formulaire d'avis de changement d'adresse, signalant aux clients qu'en signant le formulaire, ils consentaient à ce que l'information soit offerte, à des fins de correction d'adresse, aux expéditeurs détenant leur nom et leur ancienne adresse. Un complètement d'information figurait sur de la documentation connexe, mais les plaignants ont soutenu que, dans le fracas occasionné par le déménagement, il était facile de la perdre. Le fait pour une organisation de supposer qu'un client a accordé sa permission si elle n'en a pas entendu parler est une pratique commerciale commune appelée option de retrait.

Bien que, strictement parlant, il n'y ait pas eu de communication à mauvais escient (les plaignants avaient exercé leur option de retrait), l'enquêteur a examiné cette procédure avec Postes Canada. Dans le cadre des modifications qu'il a apportées au programme de changement d'adresse, Postes Canada a consenti à fournir plus de détails sur le formulaire lui-même et à mettre sur pied une ligne sans frais pour répondre aux questions des clients.

Le Commissaire ne dissimule pas qu'il n'aime pas les options de retrait comme mécanismes de consentement. Postes Canada soutient que le formulaire est déjà trop touffu pour permettre d'y insérer une case de consentement et qu'il subit les

Cas

retard, soit 38 plaintes ou 18 p. 100 du total des 578 plaintes. Enfin, en confiant à un agent subalterne presque toutes les plaintes pour lesquelles des délais sont prescrits, quelque 426 cas ont été fermés, ce qui a permis de libérer les enquêteurs d'expérience et de leur confier des dossiers plus complexes.

Ces mesures ont permis de réduire considérablement le nombre de cas datant de six mois à deux ans. Cependant, en raison du volume record de nouvelles plaintes, la masse indigeste des plaintes est simplement passée dans la catégorie des plaintes datant de 6 à 12 mois.

Commissions d'enquête Une plainte au sujet de la communication de détails personnels durant l'enquête sur la Somalie reprend une question pour laquelle le Commissaire avait formulé, dans des rapports annuels antérieurs, une recommandation à l'effet que les commissions devraient figurer dans l'annexe à la *Loi sur la protection des renseignements personnels*. Dans le présent cas, la commission d'enquête sur la Somalie a ordonné au ministère de la Défense nationale (MDN) de lui remettre pour ainsi dire tous les renseignements jugés pertinents à l'enquête, ce qui comprenait, bien sûr, un nombre considérable de renseignements personnels.

Le MDN était tenu légalement de fournir ces documents, puisque la *Loi sur la protection des renseignements personnels* prévoit la communication de renseignements exigés en vertu de mandats ou de citations à comparaître. Le Commissaire a conclu que la communication des renseignements par le MDN n'était pas irrégulière. Mais il était préoccupé, tout comme l'était le personnel du MDN, par le fait qu'un particulier perd tout contrôle au sujet de ses renseignements personnels lorsque ces derniers sont remis à la commission d'enquête.

La commission d'enquête sur la Somalie a rassemblé plus de 100 volumes de documents pour les avocats et les parties. Une fois que ces volumes sont déposés à titre de pièces d'enquête, ils peuvent être consultés par les médias. Le personnel de la Commission était sensible aux incidences, en matière de protection des renseignements personnels, que comportait la communication des renseignements non pertinents. Toutefois, il n'avait aucune obligation légale de le faire. On peut en conclure que la protection de la vie privée variera d'une enquête à une autre, en fonction des connaissances du personnel, du temps dont il dispose et de son envie de le faire.

craint, et c'est compréhensible, que le fait d'identifier un requérant puisse fausser l'intervention du ministère. Les personnes qui souhaitent obtenir une réponse facile à cette question seront déçues.

Dans certains cas, les enquêteurs ont découvert que les ministères achèment automatiquement une copie de la demande d'accès (qui identifie le requérant) au personnel du programme d'AIPRP aux fins de réponse. Dans d'autres, on a délégué à ce personnel la responsabilité d'approuver la réponse ou de communiquer directement avec le requérant pour préciser certains points ou accélérer le processus. Lorsque cela n'était pas le cas, le Commissaire a jugé que la communication enfreignait les dispositions de la *Loi sur la protection des renseignements personnels*.

En règle générale, l'identité du requérant ne devrait pas être communiquée aux personnes qui n'ont pas de raison de la connaître pour traiter la demande d'accès. Dans certaines circonstances, la communication du nom du requérant est justifiée. Cependant, le Commissariat a recommandé aux coordonnateurs des ministères de peser soigneusement les circonstances entourant chaque demande afin que le ministère ne soit pas soupçonné de manipuler sa réponse.

Simplification du processus d'enquête Le Commissariat continue de revoir et de simplifier ses propres démarches. Ainsi, durant l'année, la Direction des enquêtes a été refondu en deux secteurs, l'un chargé de faire enquête sur les plaintes concernant la collecte, l'utilisation et la communication par le gouvernement des renseignements personnels, l'autre chargé de traiter les plaintes en matière d'accès. Il a aussi mis en oeuvre un système de traitement accéléré pour alléger le fardeau administratif et documentaire et réduire le temps de traitement. En outre, il a adopté des normes de qualité du service pour réduire les ressources et le temps de traitement, améliorer la qualité des enquêtes et assurer des constatations plus uniformes; une formation interne a été offerte pour assurer l'uniformité et rehausser les habiletés des enquêteurs. La Section des affaires publiques a pris en charge le traitement des demandes de renseignements afin de permettre aux agents de la Direction des enquêtes de concentrer strictement leurs efforts sur les enquêtes concernant les plaintes.

On éponge l'arrière de travail Pour réduire l'arrière de 1 629 plaintes reportées de l'année précédente, le Commissariat a pris plusieurs mesures. Après avoir repéré les plaintes remontant à plus de douze mois, qui s'élevaient au total à 578 plaintes, soit 35 p. 100 des plaintes actives, il a mis sur pied une section chargée d'éponger l'arrière; cette section était parvenue, à la fin de 1996, à clore 375 enquêtes, soit 65 p. 100 des enquêtes en cours. Il a aussi affecté d'autres employés professionnels aux enquêtes; ces employés ont répondu au reste des plaintes en

Une fois de plus, le nombre de plaintes reçues durant l'année a atteint un nombre record, soit 2235 par rapport aux 1625 reçues l'année dernière et aux 1700 plaintes prévues. Pour diverses raisons, entre autres un processus accéléré de traitement, un octroi ponctuel de fonds par le Conseil du Trésor pour l'embauche de personnel contractuel (l'argent, autant que le personnel, sont maintenant chose du passé) et un réaménagement de l'effectif, les enquêteurs ont pu fermer 2717 dossiers. En outre, un plaignant a retiré 248 plaintes, ce qui a libéré deux enquêteurs.

Les efforts du Commissariat pour résoudre les plaintes à l'étude, dont le volume est grand, sont contrebalancés par le nombre élevé de nouveaux cas; les enquêteurs gèrent en moyenne 90 plaintes en tout temps, ce qui constitue en soi une charge de travail excessive. Ils consacrent trop de temps à gérer les dossiers et à apaiser les plaignants. L'ensemble du processus avance au ralenti à cause du volume de travail, des ressources inadéquates et des réductions effectuées par le gouvernement dans les sections du programme de l'accès à l'information et de la protection des renseignements personnels (AIPRP).

Retards Le fait est que les retards sont devenus chose courante dans certains ministères en raison de l'augmentation du volume et de la complexité croissante des demandes, et à cause des réductions de personnel. Le problème date de 1983, lorsque les ministères ont été avertis qu'aucune nouvelle ressource ne serait affectée au traitement des demandes présentées aux termes de la Loi sur la protection des renseignements personnels et de la Loi sur l'accès à l'information, qui venaient d'être adoptées.

Depuis, en dépit de la baisse constante des ressources humaines, les organismes fédéraux ont répondu à plus de 650 000 demandes. À moins qu'il n'y ait un incitatif technologique, il n'y a pas de fonds disponibles, bien que ce travail exige une main-d'œuvre considérable. Les gestionnaires peuvent accroître l'efficacité jusqu'à un certain point, après quoi les fonctions doivent être reportées, réduites ou éliminées. Le programme de l'AIPRP, qui n'est pas une fonction de base des ministères, se retrouve souvent au haut de la liste des réductions à effectuer. Il en résulte un service de moindre qualité, et l'efficacité et la crédibilité du programme en souffrent.

Identification du requérant Le fait de divulguer au personnel d'un ministère ou d'un organisme l'identité d'une personne présentant une demande d'accès à l'information constitue-t-il une infraction à la protection des renseignements personnels? Difficile question, dont le Commissariat a été de nouveau saisi. On

conforme des données, mais pas son extension à d'autres ministères. Le personnel d'Agriculture a compris et le projet de couplage des données qu'il a éventuellement soumis se limitait au projet original particulier.

Autres projets de couplage des données

Le personnel du Commissariat a aussi étudié deux autres projets de couplage des données; l'un de ces projets, celui de Ressources humaines Canada (RHC) concernant le couplage des prêts pour étudiants, est en cours.

Ressources humaines cherche les personnes n'ayant pas remboursé leurs prêts aux étudiants Pour recouvrer les sommes dues au gouvernement, RHC a demandé à Travaux publics et Services gouvernementaux Canada de confronter sa liste des débiteurs défaillants aux données de la base de données des fonctionnaires fédéraux. Travaux publics a abordé cette demande avec le Commissariat.

Le personnel du Commissariat a fait remarquer que, bien que Travaux publics administre les listes de paye et d'avantages sociaux, il le fait au nom du Conseil du Trésor, qui est l'employeur de la fonction publique. C'est le Conseil du Trésor, en qualité de véritable propriétaire des données, qui serait tenu d'être d'accord avec RHC pour qu'un projet de couplage soit soumis. En dépit de ses garanties verbales répétées que le Conseil du Trésor était d'accord, RHC n'a pu produire d'autorisation écrite. Comme le Commissariat ne souhaitait pas examiner le projet sans le consentement du Conseil du Trésor, la question était en suspens à la fin de la période couverte par le présent rapport.

Agriculture Canada compense les dettes des fermiers par rapport aux prestations Agriculture Canada a proposé d'appartier les demandes de prestations des propriétaires fonciers pour deux programmes, soit le programme relatif aux paiements supplémentaires pour les terres labourables et le programme d'aide à la mise en commun des frais de transport, et les listes des fermiers qui doivent de l'argent aux termes d'autres programmes d'Agriculture et Agro-alimentaire Canada et de la Commission canadienne du blé. L'analyse des coûts et avantages a permis de calculer que le montant à recouvrer s'élève à environ 900 000 dollars, et que les coûts sont négligeables puisque le logiciel est déjà configuré pour appartier les données.

L'appariement n'est pas décrit en termes spécifiques aux requérants du programme des terres labourables; toutefois, le personnel d'Agriculture a soutenu que l'extinction d'obligations est décrite comme une condition du programme sur le formulaire de demande et dans la lettre qui précise le montant dû.

Il semblerait qu'à un certain moment Agriculture envisageait d'étendre l'appariement à d'autres ministères auxquels des sommes sont dues, comme Revenu Canada et Anciens Combattants. Le Commissariat pouvait accepter un couplage de données particulier à l'intérieur d'un ministère à titre d'utilisation

visés ne soient étudiés et qu'il soit établi si la divulgation de leur contenu, si contenu il y a, peut être préjudiciable.

Il semblerait que le ministre poursuive sa demande de désignation et le Commissaire maintiendra son opposition.

Communications dans l'« intérêt public »

La Loi sur la protection des renseignements personnels interdit en général aux ministères et organismes fédéraux de communiquer les renseignements personnels de leurs employés et clients, mais elle prévoit plusieurs circonstances dans lesquelles une communication peut être justifiée. L'une des dispositions concernées, l'alinéa 8(2)m), autorise le responsable d'une institution à communiquer les renseignements s'il juge que l'intérêt public l'emporte sur toute intrusion dans la vie privée. Il doit alors notifier le Commissaire à la vie privée, lequel avertira à son tour les personnes touchées, le cas échéant.

Dans le passé, ce sont le Service correctionnel du Canada, la Commission nationale des libérations conditionnelles (CNLC) et la Gendarmerie royale du Canada (GRC) qui ont le plus souvent invoqué cette disposition pour communiquer des rapports sur des incidents impliquant des détenus et des libérés conditionnels, et, dans le cas de la GRC, signaler à une collectivité la libération imminente d'un dangereux criminel.

Le nombre de notifications a légèrement baissé cette année; il est passé de 69 à 63 demandes en raison du nombre moins élevé de demandes présentées par la CNLC. Toutefois, le nombre de notifications de la GRC a augmenté de douze depuis les trois dernières années; la hausse est attribuable en partie au fait que le pouvoir de communication a été délégué par l'administration centrale aux commandants de division, et que la question de la sécurité de la population soulève le tollé général.

Neuf des notifications signalaient la libération de criminels violents dans des collectivités du Manitoba après examen par le nouveau Comité consultatif de notification aux collectivités du Manitoba. La GRC a élaboré sa propre politique au sujet de l'arrivée de criminels violents ou dangereux, et plusieurs provinces ont établi des comités chargés d'examiner ces notifications de façon plus systématique, ou sont sur le point de le faire.

Désignation d'un nouvel « organisme d'enquête »

Le ministère de la Justice a sollicité l'avis du Commissaire sur la désignation possible de la Direction de la conservation et de la protection du ministère des Pêches et des Océans à titre d'« organisme d'enquête » aux termes des alinéas 8(2)(e) et 22(1)(a) de la Loi sur la protection des renseignements personnels.

Un organisme ainsi désigné est autorisé à refuser à une personne l'accès à ses renseignements personnels pendant une période pouvant atteindre vingt ans, si les renseignements ont été recueillis dans le cadre d'une « enquête licite », quelque banal qu'en soit le caractère, ou si la communication des renseignements peut nuire à l'enquête. En termes légaux, il s'agit d'une « exception objective », qui a l'avantage, tout au moins pour l'organisme en question, de ne pas obliger le personnel à ouvrir les dossiers en réponse à une demande d'accès. La divulgation n'est pas obligatoire.

Le Commissaire n'a pas mâché ses mots. Tout en reconnaissant qu'il doit y avoir équilibre entre le droit d'accès de l'individu et le besoin pour l'État de maintenir le secret, il a néanmoins jugé inacceptable que ce principe trouve son expression dans une disposition législative qui ne renferme pas de critères de préjudice. Il a qualifié de répugnant l'alinéa 22(1)(a).

En dépit des constatations favorables d'une étude que le ministère de la Justice a fait en 1996 de l'utilisation par les ministères de l'alinéa 22(1)(a), le Commissaire a noté que le caractère discrétionnaire de l'application de l'exemption générale est trop rarement invoqué. Il a donné des exemples de dossiers exemptés qui contenaient des coupures de presse, et de la correspondance entre le ministère et le sujet. Le Commissaire a reconnu que le recours à l'alinéa 22(1)(a) rend la vie des fonctionnaires plus facile, mais il a ajouté que la commodité administrative ne devrait pas être une considération.

Le cas particulier était particulièrement troublant en ce sens que le ministère, dans sa demande, tentait aussi d'obtenir une exemption générale semblable aux termes de la Loi sur l'accès à l'information. Un organisme peut avoir de bonnes raisons de solliciter une exception objective pour rejeter un droit général d'accès aux termes de la Loi sur l'accès à l'information (question qui relève de la compétence du Commissaire à l'information), mais le ministère n'a pas prouvé, dans sa demande, qu'il devait être autorisé à refuser à un particulier l'accès à ses renseignements personnels aux termes de la Loi sur la protection des renseignements personnels, ce qui constitue, pourrait-on soutenir, un critère plus astreignant. Un exemption ne devrait certes pas être invoquée sans que les dossiers individuels

Le personnel du Commissariat a suggéré de légers ajustements (qui feront l'objet d'un suivi), mais il n'a relevé aucune faiblesse importante sur le plan de la protection des renseignements personnels. Il a conclu qu'une vérification plus approfondie est inutile, compte tenu surtout du rôle atténué que joue le gouvernement dans les prêts consentis aux termes du nouveau programme.

Commission des plaintes du public de la GRC

La Commission est un organisme indépendant qui examine la façon dont la GRC fait enquête sur les plaintes portées contre ses membres. Elle peut aussi recevoir des plaintes directement du public, qu'elle renvoie toutefois à la GRC aux fins d'enquête. La Commission a des bureaux régionaux à Vancouver et à Edmonton, mais l'examen de toutes les plaintes se fait à l'administration centrale, située à Ottawa.

Le personnel du Commissariat a jugé que la Commission était en général respectueuse des dispositions de la *Loi sur la protection des renseignements personnels*; il a recommandé que la Commission :

- obtienne le consentement pour la communication, dans ses rapports, des renseignements personnels qui servent, sans être requis, pour le déroulement de l'enquête;
- modifie la description des banques de renseignements personnels pour mieux en décrire les fonds et signaler les périodes de conservation et d'élimination des renseignements;
- détruise les dossiers d'emploi des anciens employés lorsque la période d'élimination approuvée est dépassée, et les évaluations des employés actuels datant de plus de cinq ans;
- conservent dans ses fonds de renseignements les notes prises par les membres.

La recommandation concernant la conservation des notes prises par les membres pourrait être affectée par la décision de la Cour d'appel fédérale dans la cause relative à l'accès aux notes des membres du Conseil canadien des relations de travail (voir à la page 47).

La vérification a aussi permis de relever des données personnelles se trouvant sur les ordinateurs de bureau de SNA, dont 3 500 ont été transférées à NAV CANADA. Les gestionnaires qui tiennent les dossiers d'emploi sur ces ordinateurs ont été priés de retirer les données des personnes qui n'avaient pas été transférées. Transports Canada déterminera les limites d'accès aux gros ordinateurs et aux réseaux lorsque les employés de Transports et de NAV CANADA partageront temporairement des bureaux et des systèmes informatiques.

NAV CANADA a maintenant reçu les renseignements personnels dont elle a besoin pour gérer les employés qui ont accepté son offre d'emploi. Transports Canada conservera tous les autres dossiers, soit ceux des employés qui ont refusé leur transfert, ainsi que les renseignements désuets qui ont été retirés des dossiers. La bonne nouvelle : une partie considérable des dossiers de Transports Canada (et presque tous les dossiers de personnel de NAV CANADA) ont fait l'objet d'un bon nettoyage. Peut-être que les résultats inciteront le ministère à revoir le reste de ses dossiers. Certains problèmes qu'a connu Transports Canada auraient pu être évités ou minimisés si NAV CANADA avait été assujéti aux dispositions de la Loi sur la protection des renseignements personnels. Le fait d'attendre que le processus de privatisation soit en cours avant de traiter les questions liées à la protection des renseignements personnels n'a fait qu'exacerber le problème. Le fait de demander dès le début du processus la participation du Commissariat est une solution, mais en fin de compte, il vaut beaucoup mieux assujettir ces nouvelles entités aux dispositions de la Loi sur la protection des renseignements personnels.

Programme canadien de prêts aux étudiants

Le programme est administré par Ressources humaines Canada. Il assure des subsides aux taux d'intérêt aux institutions financières pour qu'elles fournissent des prêts aux étudiants admissibles, mais il ne garantit pas le remboursement des prêts approuvés depuis que le nouveau programme canadien d'aide aux étudiants a adopté. Les prêts consentis aux termes de l'ancienne Loi canadienne sur les prêts aux étudiants demeurent garantis par le gouvernement fédéral. Dans les deux cas, les prêts non remboursés sont remis aux mains d'agences de recouvrement. La vérification a porté sur les listes publiques dans *Info Source*, le partage de l'information, la sensibilisation du personnel à l'égard des questions de protection des renseignements personnels, les méthodes contractuelles, la sécurité, l'utilisation des télécommunications pour transmettre les renseignements personnels et des ordinateurs pour traiter et stocker les données.

Toutefois, le problème le plus pressant était la date du 1^{er} novembre 1996, où se ferait le transfert du système à NAV CANADA; cette date était trop rapprochée pour que l'on puisse accomplir l'examen qui était manifestement nécessaire. Le Commissaire à la vie privée a écrit au sous-ministre de Transports Canada pour lui signaler ses constatations préliminaires. Transports Canada a consenti à reporter de 60 jours la date de transfert projeté des dossiers personnels et a embauché 35 commis temporaires pour revoir les dossiers et les purger de l'information sans rapport avec NAV CANADA.

Au cours de leur recherche préliminaire, le personnel a découvert que tous les dossiers personnels, ou presque, contenaient des renseignements au sujet d'autres personnes, entre autres des noms, des numéros d'assurance sociale, etc., souvent sous forme de listes, mais aussi sous forme de fiches de temps supplémentaires, de listes de retenues à la source, de notes de services, de formulaires. Une grande partie des renseignements concernaient des personnes qui n'étaient plus des employés ou qui n'étaient pas touchées par le transfert; les renseignements les touchant n'étaient donc pas pertinents à NAV CANADA. En plus, bien sûr, toutes ces personnes n'avaient pas consenti à la communication de ces renseignements. Transports Canada a consenti à supprimer les renseignements non pertinents.

Le ministère a aussi accepté de détruire nombre de documents, se trouvant dans les dossiers du personnel et les dossiers de travail des gestionnaires, qui ne servaient plus à des fins administratives et qui auraient dû être détruits depuis longtemps. Ces documents comprenaient de vieilles mesures disciplinaires, des griefs résolus, des formulaires de paye et de taxe, des renseignements au sujet de congés familiaux, des certificats de médecin à l'appui de congés de maladie.

Les dossiers d'évaluation de la région du Québec contenaient aussi des déclarations de conflit d'intérêt et des attestations aux termes du code d'après-mandat, qui ne s'appliquaient pas à NAV CANADA. L'Institut de formation de Cornwall détenait des renseignements sur les candidats retenus et sur ceux qui avaient échoué ou abandonné leurs cours (nombre de ces candidats n'étaient pas des employés du SNA); certains renseignements dataient de 1959. Tous ces renseignements ont été retirés et remis à la direction de la gestion de l'information de Transports Canada aux fins de stockage ou de destruction.

Résultats : Le personnel de Transports a retiré presque un million de pages de renseignements personnels des dossiers ou non pertinents des dossiers qui allaient être transférés. Cela représente 330 boîtes d'entreposage courantes; emplies, ces boîtes atteindraient une hauteur de 32 étages. Tout bien penser, les gestionnaires des dossiers de NAV CANADA devraient être pleins de gratitude.

Le Commissariat s'est beaucoup moins appuyé sur les vérifications comme méthode pour évaluer le respect des dispositions de la *Loi sur la protection des renseignements personnels*. La tenue de vérifications systématiques s'est avérée irréalisable compte tenu des ressources plus rares dont dispose le Commissariat. Le personnel a mené deux vérifications courantes au cours de l'année, qui ont porté sur le programme de prêts aux étudiants de Ressources humaines Canada et sur la Commission des plaintes du public de la Gendarmerie royale du Canada. Une troisième vérification, portant sur les fichiers du système de navigation aérienne de Transports Canada, a été faite avant le transfert à NAV CANADA.

Transports Canada - Nav Canada

Le transfert du système de navigation aérienne (SNA) est l'un des plus gros projets de commercialisation entrepris par le gouvernement. Le SNA comprend sept centres de contrôle régionaux, 44 tours de contrôle, 88 stations d'information de vol et un réseau d'aides à la navigation. Il gère l'ensemble de l'espace aérien national et l'espèce aérien désigné de l'Organisation de l'aviation civile internationale dans la région de l'Atlantique nord; il assure le contrôle de la circulation aérienne pour environ 6,8 millions de mouvements d'aéronefs chaque année. En vertu de l'accord, NAV CANADA a acheté tous les biens pertinentes et a assumé la responsabilité d'environ 6 400 employés.

Au milieu de l'année 1996, le Commissaire à la vie privée a comparu devant le Comité de la Chambre des communes sur les services de transport et a insisté pour que NAV CANADA soit assujéti aux dispositions de la *Loi sur la protection des renseignements personnels* afin d'assurer le maintien de la protection des renseignements personnels des clients et employés. Le Comité a accepté cet avis et a recommandé que le gouvernement incorpore cette disposition dans la loi habilitante. NAV CANADA a résisté, le gouvernement a délaissé la recommandation et la loi a été adoptée sans avoir été révisée.

Compte tenu de la taille du système et de la possibilité de la communication de vastes quantités de renseignements personnels, le Commissaire a entrepris une vérification du transfert à NAV CANADA. En août 1996, le personnel a commencé à examiner les dossiers dans les bureaux de la capitale nationale et de la région du Québec, des tours de contrôle d'Ottawa et de Dorval, et de l'Institut de formation de Cornwall. Il a relevé plusieurs problèmes, y compris l'existence de renseignements personnels désuets, de renseignements dont NAV CANADA n'avait pas besoin et, dans certains cas, de renseignements de nature confidentielle se trouvant dans les dossiers de travail des gestionnaires, renseignements qui n'auraient pas dû être recueillis en partant.

L'archiviste en chef a pris en considération toutes les recommandations du Commissaire et remis à plus tard la vente des radiographies jusqu'à ce que l'on soit en mesure d'en faire une opération rentable. Entre-temps les radiographies seront détruits dans de l'équipement de la GRC approuvé.

place à confirmer que les palettes avaient été placées dans l'aire de déchargement et qu'on lui avait dit de les y laisser, car quelqu'un devait venir ramasser le tout. Il a aussi confirmé que, lorsque l'entrepreneur s'était présenté, ce dernier avait ouvert une ou deux enveloppes et avait été surpris d'y trouver des dossiers médicaux alors qu'il croyait n'avoir acheté que des radiographies.

L'entrepreneur a aussi confirmé que les 300 enveloppes traitées, sauf deux, contenaient des rapports médicaux, la plupart agrafées à l'extérieur. Lorsque les documents ont été retournés au Centre des documents, on a trouvé des centaines de radiographies, des enveloppes et des rapports médicaux, ainsi que plus de 60 paquets contenant chacun en moyenne de 40 à 45 enveloppes de radiographies. Le Centre a comparé les documents retournés aux listes des acquisitions pour s'assurer que tous les documents y étaient.

L'enquêteur a confirmé qu'en plus des films radiographiques, les documents renfermaient des renseignements médicaux de nature confidentielle concernant des immigrants éventuels au Canada, y compris des photos de candidats, des rapports médicaux préliminaires, des rapports de radiologie ainsi que des résultats de tests de laboratoire sur l'état médical, entre autres sur la possibilité de maladies infectieuses ou transmises sexuellement. L'enquête a aussi permis de confirmer que des renseignements personnels (nom, numéro de passeport, date de naissance, adresse, etc.) figuraient sur les radiographies.

Le Commissaire a jugé que les agents locaux du Centre fédéral des documents de la région du Manitoba avaient été négligents dans le traitement des documents et la vente des radiographies. La remise de ces documents à l'entrepreneur entraînait clairement la *Loi sur la protection des renseignements personnels*. Le Commissaire a fait plusieurs recommandations à l'archiviste en chef, notamment :

- suspendre toutes les ventes de radiographies jusqu'à ce que de nouvelles procédures soient mises en place;
- retirer les films radiographiques des enveloppes, détruire ces enveloppes et toute marque d'identification;
- exiger des entrepreneurs et du personnel ayant accès aux radiographies qu'ils signent une entente relative au maintien de la confidentialité;
- sensibiliser le personnel du Centre des documents à ce qui constitue des « renseignements personnels » et à l'obligation qui lui est faite de les protéger;
- signaler sans délai au Commissaire tout autre incident semblable dans l'avenir.

Il semble que les dossiers médicaux avaient été entreposés au Centre de documents des Archives nationales à Winnipeg aux fins d'élimination; après un examen superficiel, comme ils ne semblaient contenir que des radiographies, il avait été décidé de les vendre par l'intermédiaire des Biens de la Couronne à un entrepreneur local pour l'extraction du nitrate d'argent. Cependant, plutôt que remettre les seules radiographies, les Archives avaient envoyé les enveloppes contenant les dossiers médicaux de plus de 2 600 immigrants éventuels au Canada.

L'entrepreneur, qui avait acheté les radiographies pour en extraire le nitrate d'argent, s'était retrouvé avec une masse de documents et beaucoup plus de travail qu'il n'en escomptait. Il avait dû ouvrir environ 300 dossiers pour séparer les radiographies des autres documents; une fois le tri effectué, il avait jeté aux ordures les documents qui étaient sans intérêt pour lui. Lorsque les journalistes du *Winnipeg Free Press* étaient arrivés sur les lieux pour prendre des photos, il avait réalisé que ces documents n'auraient pas dû être jetés aux ordures et il avait été sans tarder les récupérer.

L'entrepreneur avait été troublé par l'article paru à ce sujet et les appels provenant de divers agents gouvernementaux, mais après des pourparlers avec l'agent de vente du Centre de distribution des biens de la Couronne, les Archives nationales et l'enquêteur, il avait décidé de remettre tous les documents et les radiographies aux Archives.

Santé Canada avait entériné la décision d'éliminer les dossiers périmés, tout comme les Archives nationales avaient convenu que les radiographies d'immigrants éventuels n'avaient aucune valeur historique. Parce qu'il croyait que les dossiers contenaient seulement des radiographies, le gestionnaire du Centre des documents avait expédié ce qui était décrit comme « 1 200 livres de radiographies—nitrate d'argent récupérable » aux Biens de la Couronne, où l'offre de l'entrepreneur avait été acceptée.

Un membre du personnel des Archives a dit à l'enquêteur qu'il avait ouvert plus de dix enveloppes et n'y avait trouvé que des radiographies, et pas de rapports médicaux. Il s'était assuré que les enveloppes ne portaient pas de numéro d'assurance sociale ou d'adresse et qu'il n'y figurait que le nom de la personne et, dans certains cas, un timbre sur lequel avaient été notés des renseignements médicaux, qu'il avait jugé non confidentiels. Il avait marqué les documents à éliminer comme rebut non classifié, et le tout avait été transporté à l'aire de déchiquetage. D'autres employés avaient vu les documents—dossiers médicaux et photographies agrafés à l'extérieur des enveloppes—et avaient supposé que le tout était à déchiqueter. Un superviseur de l'entreprise de déchiquetage qui était sur

Selon l'article, quelque 300 originaux d'examen médicaux préliminaires de personnes demandant d'être admises au Canada avaient été trouvés dans des bacs à ordures débordants dans une allée à Winnipeg. Les documents, qui remontaient aux années 1970 et au début des années 1980, reposaient intacts dans des enveloppes de Santé et Bien-être Canada et incluaient des photos, des radiographies et des renseignements médicaux personnels.

Les documents avaient été déposés dans deux bacs à ordures à l'arrière d'une maison en rangée. Les sacs de plastique s'étaient déchirés, et une partie de leur contenu s'était répandue sur le sol. Une résidente les avait ramassés et remis dans le bac; puis elle avait communiqué avec les agents d'Immigration Canada à l'Aéroport international de Winnipeg dans l'espoir qu'on vienne les chercher. Insatisfaite de la réponse obtenue, elle avait alors communiqué avec le *Winnipeg Free Press*, puis avec la police.

L'enquêteur a recueilli le témoignage de plusieurs parties et établi les faits. Un agent de la Citoyenneté, qui travaillait tard le 6 mai, avait reçu un appel d'un agent de l'Immigration à l'Aéroport international de Winnipeg l'informant qu'une personne avait téléphoné et signalé avoir trouvé une quantité importante de documents médicaux d'immigration dans des bacs à ordures. L'agent de la Citoyenneté s'était alors rendu sur les lieux.

Il avait trouvé deux bacs à ordures remplis d'enveloppes contenant des radiographies et d'autres documents médicaux, certains avec photos. Tous les documents semblaient concerner des personnes ayant demandé le statut d'immigrant au Canada. Certains portaient l'identification de Santé et Bien-Être. N'ayant pu trouver un agent de ce ministère, l'agent avait alors contacté le gestionnaire de Citoyenneté et Immigration Canada à Winnipeg pour lui signaler la découverte; il l'avait par la suite rappelé pour l'avertir que les bacs devaient être vidés le lendemain matin.

Le lendemain matin, deux employés de Santé Canada avaient appris l'affaire par le journal. Ils s'étaient rendus sur les lieux pour ramasser les documents. Leurs recherches les avaient amenés à inspecter les bacs à ordure de trois pâtés de maisons, à tenter de localiser le camion à ordures, qui avait déjà vidé un bac, et finalement à se rendre au site d'enfouissement. Ces employés, accompagnés de deux autres employés, avaient fouillé la zone où le camion avait déchargé son contenu, mais ils n'avaient rien trouvé. Comme des tracteurs de la municipalité avaient enterré les ordures déchargées et nivelé la zone, il semblait peu probable que les documents soient encore accessibles.

payait avec sa carte de crédit, mais il n'avait pas commandé la série de l'Oursou Winnie. Les timbres, facturés à son compte de crédit, lui avaient été envoyés, accompagnés d'une note expliquant que l'envoi pouvait être retourné contre crédit s'il ne désirait pas le conserver.

Un journaliste avait appelé pour savoir si l'utilisation abusive d'un numéro de carte de crédit fourni pour des achats spécifiques constituait une infraction à la Loi sur la protection des renseignements personnels. Bien que le Commissariat n'ait pas reçu de plainte officielle à ce sujet, Postes Canada en avait reçu 150.

Le personnel affecté à la protection des renseignements personnels a entrepris de résoudre le problème de façon informelle. Dans un premier temps, il a fallu amener le personnel de vente de Postes Canada à reconnaître que l'utilisation à mauvais escient d'un numéro de carte de crédit est une question touchant à la protection des renseignements personnels. Le personnel de vente a admis cette erreur de marketing, mais il a fallu le convaincre que le fait d'utiliser des renseignements recueillis à une fin à une autre fin, sans le consentement du client, enfreint les principes de collecte de données de la Loi sur la protection des renseignements personnels. Le coordonnateur de la protection des renseignements personnels de Postes Canada a entrepris d'expliquer ces principes au personnel de vente.

Dans un deuxième temps, on a traité des questions de permutation et d'agencement des listes de clients. Nombre de philatélistes obtiennent par commande permanente tous les nouveaux timbres, qui sont portés automatiquement à leur compte de crédit. Certains ont signé une commande pour un sujet particulier (enveloppes premier jour, timbres commémoratifs, timbres avec couronne, etc.); ils ne tiennent pas nécessairement à ce qu'on leur signale les autres produits. D'autres préfèrent décider de façon ponctuelle. Les listes de commandes permanentes n'étaient pas toujours claires; elles avaient besoin d'être épurées, et les options devaient être précisées.

Suite à cet incident, pour éviter d'expédier et de facturer des produits non sollicités, le personnel de vente de Postes Canada a communiqué avec tous ses clients ayant une commande permanente afin de leur expliquer l'éventail des produits et de leur demander de préciser à quoi ils veulent souscrire.

Dossiers de Santé Canada jetés aux ordures à Winnipeg

À la suite d'un appel d'un journaliste concernant la découverte à Winnipeg de dossiers médicaux et d'enveloppes contenant des radiographies dans un bac à ordures, un enquêteur du Commissariat a été dépêché sur les lieux.

Archives nationales en vue d'adopter un calendrier approprié et de décrire dans *Info Source*, le répertoire des fichiers de renseignements que détient le gouvernement fédéral, les fonds de renseignements qu'il détient.

La Société canadienne des postes copie les adresses des clients de ses compétiteurs

Un autre journaliste avait signalé qu'une campagne pour mousser les ventes avait lieu à la succursale postale de Longueuil, près de Montréal. Il semble que, dans son enthousiasme, le personnel de vente avait incité les trieurs du courrier et les facteurs à photocopier ou noter les adresses figurant sur les enveloppes de neuvi entreprises de messagerie. Le personnel de vente prévoyait de se servir des adresses ainsi obtenues pour approcher les clients de ses compétiteurs et tenter de leur vendre les services de Postes Canada.

En guise d'encouragement, un dollar par client éventuel serait versé dans les cagnottes des unités respectives et une récompense de 50 \$ serait tirée parmi le personnel participant.

L'agent de portefeuille a communiqué avec Postes Canada, qui a reconnu immédiatement que la promotion était inacceptable et que la haute direction prenait la chose très au sérieux. Pour déterminer si cette promotion constituait une infraction à la *Loi sur la protection des renseignements personnels*, la question était de savoir s'il s'agissait d'adresses domiciliaires plutôt que d'adresses et de titres d'entreprises.

Pendant que l'enquête se déroulait, la Ministre a été interrogée sur l'incident à la Chambre des communes. Elle a répondu que la promotion était une erreur et constituait un incident isolé, qui ne se reproduirait pas. Le président de la Société canadienne des postes a obtenu de tous les vice-présidents l'assurance par écrit que ce n'était pas une pratique courante. Le gestionnaire et les trois employés affectés à la vente seront tenus de suivre un cours d'éthique et de signer une déclaration à l'effet qu'ils reconnaissent avoir suivi et compris le cours.

En raison de la réaction rapide et énergique de Postes Canada, le Commissaire a déclaré la plainte résolue. Toute autre plainte individuelle sera traitée de la façon habituelle.

Philatéliste facturé pour des produits non commandés

Une autre pratique commerciale de la Société canadienne des postes a froissé un philatéliste : des timbres qu'il n'avait pas commandés avaient été portés à son compte de crédit. Il achèterait à l'occasion des produits de Postes Canada, qu'il

Documents de vérification fiscale trouvés dans un classeur excédentaire

Un journaliste d'une station de radiodiffusion avait signalé que plusieurs dossiers d'impôt avaient été trouvés dans un vieux classeur. Il en avait fait deux copies, l'une pour l'avocat de la station, l'autre à l'intention du Commissaire. Les originaux avaient été retournés à la personne qui les avait découverts, et celle-ci les avait fait suivre à son député.

L'examen mené par le Commissariat a permis d'établir qu'il s'agissait de dossiers de vérification fiscale qui renfermaient aussi des documents de transactions bancaires et immobilières d'environ neuf personnes. L'enquêteur a retourné les dossiers à Revenu Canada et ouvert une enquête.

Il semble que le classeur en question faisait partie d'un lot de 275 classeurs envoyés entre mars et juin 1996 par le Bureau de services fiscaux de North Toronto au Centre de distribution des biens de la Couronne aux fins de vente. Les classeurs avaient été déclarés excédentaires à la suite d'un réaménagement important des locaux, entrepris pour maximiser l'espace et accueillir du personnel de la TPS provenant d'un autre immeuble. Les employés touchés par le déménagement avaient été temporairement réinstallés sur d'autres étages, et les classeurs excédentaires rassemblés en vue d'être vendus. L'acheteur s'était procuré le classeur en question au Centre de disposition de Mississauga et, en l'ouvrant, y avait trouvé des documents dans le premier tiroir, puis derrière une cloison dans un autre tiroir. Ebranlé par cette négligence, il avait alors communiqué avec le journaliste.

Il est fort probable que ce classait faisait bien partie du lot des 275 classeurs de North Toronto mais le personnel n'a pas été en mesure de le déterminer avec certitude. Lors du déménagement, il avait été appelé aux employés de vérifier soigneusement les classeurs; une vérification ponctuelle avait été menée, mais tous les classeurs n'avaient pas été ouverts. Même s'il s'agit sans nul doute d'une erreur humaine, Revenu Canada a néanmoins revu ses procédures administratives et les a renforcées pour éviter que cela ne se reproduise.

Le Commissaire a demandé à Revenu Canada d'avertir les contribuables concernés, de présenter ses excuses et d'expliquer ce qui s'était passé. Il a aussi fait remarquer que les dossiers eux-mêmes contenaient de vieux documents de travail qui ne faisaient pas partie des dossiers officiels de vérification. Il semble que Revenu Canada n'ait pas de calendrier de délais de conservation et qu'une élimination des documents et que certains documents étaient conservés indéfiniment. Le Commissaire a demandé à Revenu Canada de consulter les

renseignements détenus par le gouvernement et la protection de la vie privée des personnes visées par certains de ces mêmes renseignements. La Cour a reconnu la prépondérance qu'accordent tant la *LAI* que la *LPRP* à la protection de la vie privée une fois que des renseignements sont considérés "personnels" au sens de l'article 3 de la *LPRP*. Les juges ont de plus décrété que le début de cette définition ("[...] renseignements [...] concernant un individu identifiable [...]") primait en importance lorsque venait le moment de déterminer si un renseignement est personnel. Ainsi que le dit le juge La Forest, "[e]n conséquence, si un document de l'administration fédérale est visé par cette disposition liminaire, il importe peu qu'il ne relève d'aucun des exemples donnés".

La vaste définition sciemment adoptée par la Cour reflète les grands efforts du législateur en matière de protection des libertés individuelles. Pour reprendre les propos du tribunal, "[e]lle semble destinée à viser **tout** renseignement sur une personne donnée, sous la seule réserve d'exceptions précises [...] Une telle interprétation s'accorde avec le texte clair de la Loi, avec son historique législatif et avec le statut privilégié et fondamental du droit à la vie privée dans notre culture sociale et juridique."

Le Commissaire à la vie privée du Canada c. le Conseil canadien des relations de travail et al. Dossier A-865-96

Dans cette cause, le Commissaire à la vie privée appuie la demande qu'un individu a présentée visant l'accès aux renseignements personnels le concernant et contenus dans les notes personnelles prises par deux des membres du Conseil canadien des relations de travail. Débouté en première instance en juin 1996, le Commissaire a porté la cause devant la Cour fédérale d'appel, laquelle doit statuer sur la définition de "renseignements personnels", la notion de contrôle d'un organisme sur ces renseignements, et la nature des exceptions prévues par la loi. La Cour doit également se pencher sur la partie d'indépendance avec les juges à laquelle prétendent les membres du Conseil.

Cet appel, qui devrait être entendu à l'automne, fait également intervenir la Commission des relations de travail dans la Fonction publique, le Tribunal des droits de la personne, le Tribunal canadien du commerce extérieur, l'Office national des transports du Canada et le Procureur général du Canada.

Michael A. Dagg c. le Ministre des Finances, le Commissaire à la vie privée du Canada et l'Alliance de la Fonction publique du Canada.
Dossier C.S.C. 24786

Suite à sa demande visant une copie des fiches d'entrée remplies par les employés du ministère des Finances en dehors des heures ouvrables, M. Dagg avait reçu les documents demandés, mais sans les noms, numéros d'identification et signatures des employés affectés. Le ministère lui ayant expliqué que ces renseignements lui semblaient personnels, M. Dagg s'était tourné vers le Commissaire à l'information du Canada, lequel avait entériné la décision du ministère.

Ayant obtenu du tribunal de première instance qu'il renverse la décision du ministère, M. Dagg devait cependant perdre en appel avant de se tourner vers le plus haut tribunal du pays. La Cour suprême du Canada lui a alors donné raison dans cette toute première cause dont elle était saisie en vertu de la *Loi sur la protection des renseignements personnels* (la "LPRP"). Cinq des neuf juges ont statué que les renseignements visés par M. Dagg se rapportaient au poste des employés et non à ces derniers, étant de ce fait exclus de la définition que la LPRP offre de l'expression "renseignements personnels", et donc accessibles en vertu de la *Loi sur l'accès à l'information* (la "LAI").

Cette décision est fondamentale de par son rôle de phare éclairant la réconciliation de deux objectifs apparemment ennemis, soient l'accès aux

interceptés par les détecteurs analogues. Mais l'adoption du numérique n'est pas la solution ultime.

Les signaux numériques peuvent être interceptés : les récepteurs numériques, qui sont actuellement rares et coûteux, vont devenir plus courants et économiques avec le temps. En octobre 1996, en réponse à un engagement pris antérieurement, Industrie Canada a publié la norme RSS-135-1, qui oblige l'utilisateur du récepteur numérique à obtenir une licence. Toutefois, cette obligation ne sera pas faite à l'utilisateur du récepteur numérique réglable manuellement, qui est le type de récepteur le plus vendu actuellement.

Le signal numérique codé peut être débrouillé : Le chiffrement numérique est bien meilleur que le chiffrement analogique, mais un signal numérique peut toujours être décodé, comme l'ont prouvé en mars 1997 des chercheurs de l'Université de la Californie à Berkeley et une compagnie américaine de systèmes.

Le signal numérique ne demeure pas toujours numérique : Le signal numérique est automatiquement converti en signal analogique si tout point le long du trajet de transmission ne peut l'accepter; par exemple, il sera converti si le destinataire utilise un téléphone classique ou cellulaire analogique. Dès que le signal numérique se transforme en signal analogique, il peut être intercepté encore plus facilement. (Bien sûr, toute conversation acheminée par un câble classique est protégée par les dispositions du *Code criminel* en matière d'écoute clandestine.

Ces mises en garde s'appliquent tout autant à tous les services sans fil numériques, comme les services de communications d'affaires, la radio mobile spécialisée améliorée, les systèmes de communications multipoints locaux (CellularVision Canada, MaxLink Communications et RegionalVision Canada), les téléavertisseurs, les services de communication personnelle et le téléphone sans fil.

Il a aussi incité le CRTC à interdire aux autres éditeurs d'annuaire de contacter, grâce à d'autres sources d'information, l'abonné non inscrit pour promouvoir son inscription dans leurs annuaires; il a en outre recommandé que ces éditeurs soient tenus d'établir un moyen permettant à la personne ayant accepté leur offre d'inscription dans leurs annuaires de pouvoir obtenir le retrait de son nom si elle souhaitait le faire à une date ultérieure.

Tous les services de télécommunications dressent, bien sûr, des listes de leurs clients; les compagnies vendant des téléphones cellulaires, des téléavertisseurs, des services de communication personnelle et l'Internet préparent tous des listes de clients; les sites Web commerciaux tiennent aussi des listes des visiteurs à leur site. Certaines de ces compagnies publient ou vendent leur liste. Par exemple, America On-Line a récemment vendu ses listes d'abonnés à un courtier en listes, spécialisé dans la vente des listes d'adresses à des fins commerciales.

Les fournisseurs de tels services devraient être tenus de préciser les utilisations primaires et secondaires des listes d'abonnés et d'obtenir le consentement de l'abonné pour les utilisations secondaires, comme la vente à un tiers.

Dans son rapport de décembre 1996, le CRTC était d'accord que l'abonné doit être mieux informé des options d'inscription; il a noté que la confidentialité du numéro de télécopieur et de téléphone cellulaire de l'abonné à de tels services était bien protégée par les mécanismes d'inscription existants; il a reconnu qu'en raison des frais exigés actuellement, l'abonné n'est pas incité à choisir de ne pas être inscrit. Le CRTC tiendra des audiences publiques sur les frais de non-inscription, auxquelles le Commissaire à la vie privée participera.

Se numériser : pas de solution miracle en matière de vie privée

Nombre de lecteurs se rappelleront les articles sur l'interception des conversations par téléphone cellulaire qui ont paru dans les médias. La plupart des téléphones cellulaires actuels transmettent en format analogue (ondes hertziennes classiques), et les transmissions peuvent être facilement interceptées à l'aide de récepteurs commerciaux.

Une façon d'éviter l'interception des appels cellulaires est de coder le signal pour le rendre incompréhensible à l'intercepteur. Toutefois, les signaux analogues codés peuvent être décodés sans grandes difficultés. Une autre méthode de protection consiste à transmettre le signal sous forme numérique (qui est le code binaire utilisé par l'ordinateur). Les signaux numériques ne peuvent être

Actualité en télécommunications

Inscription aux annuaires : la saga se poursuit

Nous avons signalé l'année dernière les efforts faits par des compagnies indépendantes d'édition d'annuaires téléphoniques pour acheter les listes électroniques d'abonnés de compagnies offrant un service complet. Le Conseil de la radiodiffusion et des télécommunications (CRTC) était d'accord, mais il avait demandé aux compagnies de téléphone d'offrir à leurs abonnés la possibilité de voir leur nom retirer des listes avant vente à des compagnies d'édition indépendantes.

White Directories, qui est l'une de ces compagnies, a soutenu que le fait d'offrir à l'abonné la possibilité de voir retirer son nom ferait en sorte que les annuaires des compagnies d'édition indépendantes seraient moins complets que ceux des compagnies affiliées (comme Télè-Direct, qui est l'éditeur des annuaires de Bell Canada). Elle a interjeté appel de cette décision auprès du Cabinet en alléguant que cela la désavantagerait par rapport à ses concurrents. En juin 1996, le Cabinet a renversé la décision du CRTC et il a demandé à ce dernier de lui faire rapport sur deux questions : le niveau convenable de protection à assurer aux listes d'abonnés et des mécanismes permettant aux abonnés d'obtenir la non-inscription de leurs nom et numéro. Le CRTC a sollicité des mémoires à ce sujet des parties intéressées.

Dans son mémoire de septembre 1996, le Commissaire à la vie privée a noté que la plupart des abonnés au téléphone croient comprendre que leur inscription à l'annuaire servira pour l'assistance-annuaire et apparaîtra dans l'annuaire de téléphone local. Toutefois, on ne leur dit pas que les listes sont louées et vendues à des compagnies d'édition et à des négociants, ou que leur numéro est disponible grâce à l'afficheur et lors de la mise en file d'attente avec rappel automatique. La personne désireuse que son numéro demeure confidentiel doit payer ce service de 1,55 à 5,75 dollars par mois, ce qui ne l'y incite guère.

Le Commissaire a recommandé que :

- les compagnies de téléphone précisent en détail toutes les options d'inscription à l'annuaire qui s'offre à l'abonné;
- le service de confidentialité du numéro de téléphone soit gratuit;
- l'abonné non inscrit reçoive sans frais le service de blocage de chaque ligne téléphonique; la compagnie devrait divulguer un numéro bloqué seulement en cas d'urgence et aux fins de dépistage d'appel par un organisme autorisé.

résidant. C'est la sorte de justice qui ne fait que chasser le criminel vers une autre collectivité, où il sera encore davantage incité à cacher son passé.

Juste avant que le présent rapport ne soit diffusé, le Commissaire a pris la parole lors d'une conférence nationale sur la notification de la collectivité, qui s'est tenue à Winnipeg. Les participants ont traité des conflits d'intérêt et examiné plusieurs régimes de notification, ainsi que plusieurs autres mécanismes juridiques pour protéger la sécurité du public. Nous continuerons de suivre la question de près.

En novembre 1996, la Saskatchewan a adopté la loi *The Public Disclosure Act*, qui prévoit qu'un service de police peut demander la création d'un comité de divulgation publique chargé de décider si les renseignements concernant une personne doivent être communiqués au public, et dans quelle mesure ils doivent l'être. C'est à la police qu'incombe toutefois la décision finale quant à la communication des renseignements.

En avril 1997, l'Alberta a adopté un protocole de communication des renseignements, qui s'appliquerait à toute personne déclarée coupable et jugée constituer un danger pour la population. Terre-Neuve (1996) et le Yukon (1997) ont aussi mis en oeuvre des protocoles. La *Community Safety Act* de l'Ontario, qui sert aussi à communiquer des renseignements au sujet des criminels à haut risque, a été déposée à l'Assemblée législative en 1996, mais elle n'a pas encore été adoptée.

Toujours en avril 1997, le ministère de la Justice de la Nouvelle-Écosse a publié aux fins de commentaires une ébauche de protocole sur la communication des renseignements concernant les criminels à haut risque. Le protocole prévoit la création d'un comité consultatif de notification de la collectivité, auquel la police pourrait renvoyer les cas. Toutefois, ce sont les services de police eux-mêmes, et non le comité, qui décideraient en définitive si les renseignements doivent être communiqués.

La difficulté de trouver le juste équilibre dans le débat sur la notification est illustrée par un cas récent à Ottawa. Un pédophile reconnu coupable a été libéré à la fin de sa peine d'emprisonnement. Selon les médias, le risque de récidive était considérable. Son identité a été découverte par la collectivité, et un journal a publié sa photo à la une. Peu après, le criminel a déménagé, sans que l'on sache où. En fait, il s'était tout simplement réinstallé du centre-ville à une banlieue où, en dépit de la publicité l'entourant, ses antécédents criminels sont demeurés inconnus pendant des mois.

Cela fait ressortir l'un des points faibles de la communication de l'identité d'un criminel à la collectivité. Malgré une couverture médiatique intense et la publication de sa photo, le criminel a pu se réinstaller—à tout le moins pendant plusieurs mois—dans un autre secteur de la même région métropolitaine. La publicité dans ce cas n'a pas donné grand chose et semble avoir pousser la personne à entrer dans la clandestinité.

Le même cas illustre un autre danger éventuel de la publicité. Lorsque l'identité du criminel a été enfin découverte, le criminel a été sauvagement battu par un

Diffusion de l'identité des criminels dangereux—mise à jour

Le dernier rapport annuel traitait des défis qui se posent lorsqu'on tente d'établir un équilibre entre le besoin, pour la société, de se protéger des criminels dangereux et le besoin, pour les individus ayant purgé leur peine, de réintégrer la société. Le fait de communiquer l'identité de certains criminels pourrait aider la collectivité à s'adapter à la présence de la personne, mais cette communication peut accroître le risque de danger que court la collectivité, plutôt que de la protéger.

Depuis le dernier rapport, on relève trois développements notables.

En premier lieu, le Parlement a modifié le *Code criminel*, la *Loi sur le système correctionnel et la mise en liberté conditionnelle* et d'autres lois fédérales concernant les criminels qui sont susceptibles de commettre d'autres crimes violents. Si certaines conditions sont réunies, un tribunal peut maintenant désigner de criminel à long terme une personne qui a été déclarée coupable de délits sexuels. Il doit alors ordonner que le criminel fasse l'objet d'une supervision dans la collectivité pendant une période pouvant atteindre dix ans.

Le fait de désigner criminels à long terme certaines personnes autorise et oblige la police et les responsables des services correctionnels à les superviser dans la collectivité après leur libération. Une supervision efficace par la police et les services correctionnels pourrait atténuer le besoin de signaler à la collectivité la présence, en son sein, d'un criminel.

Le *Code criminel* renferme maintenant une disposition qui autorise un procureur de la Couronne à demander au tribunal d'exiger qu'une personne signe un engagement de ne pas troubler l'ordre public, d'adopter une bonne conduite et de respecter les conditions que le juge impose. Le procureur peut invoquer cette disposition lorsqu'il a des motifs raisonnables de craindre que la personne commettra un crime grave violent. Cette disposition prévoit qu'un certain contrôle peut être exercé à l'égard des criminels dangereux qui sont libérés dans la collectivité à la fin de leur peine d'emprisonnement.

Depuis l'année dernière, plusieurs provinces ont élaboré des protocoles, ayant force exécutoire ou sous forme de déclaration de principe, établissant quand il convient de signaler à la collectivité la présence de certains criminels libérés.

la protection des renseignements personnels. Il en allait de même pour les grands ports visés par le projet de loi C-44, proposant une *Loi maritime du Canada* mais mort au Feuilleton. Et les premiers balbutiements de la future agence de perception fiscale laissent entendre un semblable assujettissement pour cette dernière.

Il nous est difficile de comprendre pourquoi des ports et une société de la Couronne telle celle des Postes peuvent tomber sous le coup de la *Loi sur la protection des renseignements personnels*, mais pas les aéroports ni les monopoles sans but lucratif tels NAV CANADA et l'Administration de la Voie maritime du Saint-Laurent. Tout est peut-être une question de temps : soit que la protection de la vie privée n'ait pas été pas à l'ordre du jour des premières privatisations, soit que notre vérification de NAV CANADA ait prouvé nos allégations. Quoi qu'il en soit, les privatisations du gouvernement fédéral respectent désormais une démarche plus systématique lorsque vient le temps de protéger la vie privée.

à la dernière minute afin de réviser tous ces dossiers (voir en page 56 pour plus de détails).

Mais pendant que notre Commissariat se concentrerait sur NAV CANADA et le GCC, le gouvernement continuait d'annoncer de nouvelles privatisations et cessions de responsabilités : les programmes de formation de la main-d'œuvre dévolus aux provinces et aux tribus autochtones; les aéroports et les ports cédés à d'autres paliers de gouvernement à moins qu'ils ne deviennent des sociétés de la Couronne; et la Voie maritime du Saint-Laurent transformée telle NAV CANADA en société privée sans but lucratif. Restent encore à venir de nouvelles agences qui inspecteront nos aliments, percevront nos impôts et surveilleront notre santé.

Le Commissaire s'est tourné vers la Greffière du Conseil Privé et le Procureur général adjoint dans l'espoir d'enrayer l'hémorragie, leur demandant de s'engager à faire protéger la vie privée lors de toute privatisation ou cession à venir, et souhaitant être tenu au courant de ces dernières dès les débuts du processus.

Le 17 mars 1997, le Commissaire recevait une lettre signée tant par le Procureur général adjoint que le Secrétaire du Conseil du Trésor, l'informant que :

"...toute entente entre un organisme fédéral et une entreprise privée découlant de la privatisation ou de commercialisation de programmes ou de services du gouvernement fédéral devrait en principe garantir le maintien de la protection des renseignements personnels affectés, et ce à un niveau équivalent à celui assuré par la Loi sur la protection des renseignements personnels. Nous sommes en train d'élaborer un énoncé de politique gouvernementale clair à ce sujet. De plus, il est logique que tout nouvel organisme fédéral soit assujéti à la Loi sur la protection des renseignements personnels, le gouvernement fédéral s'étant en effet déjà engagé à légiférer les entreprises privées relevant de sa compétence." [Traduction]

Alors que ce rapport est sous presse, et même si nous n'avons encore rien reçu en termes de politique gouvernementale, nous signalons cependant au lecteur que le ministère du Développement des ressources Humaines Canada a déployé de grands efforts afin d'incorporer le respect de la vie privée aux éléments visés par ses négociations sur la cession de ses responsabilités en matière de formation de la main-d'œuvre, ainsi qu'en témoigne l'entente fédérale avec l'Alberta sur des centres de service.

Le projet de loi C-60, créant l'Agence canadienne d'inspection des aliments, vient d'être adopté et comprend une disposition assujettissant cette dernière à la Loi sur

communication Canada (GCC). Les lettres que le Commissaire à la vie privée a envoyées aux sous-ministres de Transports Canada et de Travaux publics et Services gouvernementaux n'ont pas réussi à convaincre ces derniers de maintenir les droits à la vie privée en cause.

Lors de sa comparution devant le Comité des transports de la Chambre des communes à l'été 1996, le Commissaire a recommandé à ses membres d'assujettir NAV CANADA à la *Loi sur la protection des renseignements personnels*, ceci afin de garantir les droits à leur vie privée des personnes affectées. Le Commissaire a également exposé les risques inhérents à l'absence d'un plan bien pensé de gestion de l'information qui guentent la privatisation de toute grande opération gouvernementale. Les membres se sont dits d'accord et ont recommandé l'ajout d'une clause pertinente dans la loi habilitant NAV CANADA, ce à quoi cette dernière et le gouvernement se sont opposés, la loi entrant ensuite en vigueur sans modificatif.

Le personnel du Commissariat a proposé au GCC de l'aider dans sa révision des dossiers personnels dont hériterait le nouvel employeur, la St. Joseph Printing. Le GCC ayant accepté, les mois suivants se sont passés à préparer ces documents en prévision de la vente du Groupe. Les dossiers se limitent désormais à ceux des sociétés clientes et des employés, et ne contiennent dans ce dernier cas que les renseignements personnels de base : nom, groupe de travail, titre du poste, salaire, langue d'expression préférée et ancienne. Tous les employés visés ont attesté par écrit qu'ils n'emporteraient aucun renseignement personnel ou gouvernemental autre que les leurs. Les renseignements personnels entreposés dans les classeurs et les ordinateurs ont été transférés à un dépôt central contrôlé par Travaux publics et Services gouvernementaux, qui en assurera la conservation ou la destruction selon le cas. Tout renseignement électronique sera de plus complètement effacé avant que l'équipement informatique ne devienne la propriété de la St. Joseph.

Qui paie le musicien choisit la mélodie...

Suite à l'adoption par la Chambre des communes et le Sénat du projet de loi C-20, dépourvu de toute disposition protégeant la vie privée, le Commissaire a entrepris une vérification en vertu de l'article 37 de la *Loi sur la protection des renseignements personnels* afin de s'assurer que le transfert de renseignements personnels à NAV CANADA respectait les exigences de cette loi.

Tel que prévu, nos vérificateurs ont découvert que ce transfert serait difficile puisque la plupart des dossiers contenaient quantité de renseignements personnels superflus et que nul n'avait cherché à obtenir le consentement des individus concernés. Transports Canada a donc dû embaucher du personnel supplémentaire

Privatisations et cessions de responsabilités : Que reste-t-il ?

L'article que nous avons publié dans notre dernier rapport annuel au sujet de la privatisation de programmes fédéraux avait semé un rien de confusion : pourquoi toutes ces inquiétudes au sujet de la vie privée? Notre article traitait spécifiquement de la privatisation par Transports Canada de son groupe de contrôle de la navigation aérienne, opérant depuis sous le couvert d'une société sans but lucratif, NAV CANADA.

Le cas de NAV CANADA n'était cependant que le premier d'une série de métamorphoses fédérales, dont les diverses manifestations vont de la création d'un nouvel organisme gouvernemental à celle d'une agence entièrement privée, dont certaines sont sans but lucratif. Le dénominateur commun à chacune de ces transformations reste l'absence de dispositions assurant aux clients et aux employés affectés le maintien par le nouvel employeur de leurs droits à leur vie privée.

Au début de 1995, le Commissaire à la vie privée prévenait le législateur et la population des conséquences imprévues pouvant découler du transfert au secteur privé de responsabilités fédérales en termes de programmes ou de services. Parmi les recommandations tirées du rapport que le Commissaire remettait aux membres du Comité permanent des opérations gouvernementales, le lecteur apprendait que le législateur :

- devrait adopter une ligne directrice garantissant le maintien par la Couronne de la propriété et du contrôle (au sens de la *Loi sur la protection des renseignements personnels*) de tout renseignement personnel traité par une entreprise privée pour le compte du gouvernement;
- devrait exiger de tout organisme gouvernemental assujéti à la *Loi sur la protection des renseignements personnels* qu'il incorpore à ses contrats avec l'entreprise privée un ensemble de clauses protégeant les renseignements personnels en cause;
- devrait interdire à tout organisme gouvernemental d'amoindrir les droits à la vie privée affectés par les transactions impliquant l'entreprise privée; et
- devrait temporairement étendre l'application de la *Loi sur la protection des renseignements personnels* à tous les organismes fédéraux ainsi qu'à toutes les entreprises privées de compétence fédérale.

NAV CANADA voyait le jour peu de temps après. Le gouvernement a ensuite mis en vente ses activités d'imprimerie, assumées jusqu'alors par le Groupe

gouvernement fédéral et sur l'échange de renseignements entre les gouvernements de palier fédéral, provincial et territorial.

Le Comité recommande aussi que soit adoptée une nouvelle loi qui élargirait et renforcerait le mandat et les pouvoirs du Commissaire à la protection de la vie privée pour la protection de la vie privée au sein du gouvernement fédéral. Le Commissaire, dont le rôle se limite actuellement à traiter les plaintes et à instituer des enquêtes, serait autorisé à effectuer des vérifications, des évaluations de l'impact de la technologie et des études sur la protection de la vie privée et sur les nouvelles technologies. Le Comité recommande aussi que le Commissaire soit autorisé à revoir tout projet de loi, de règlement, de politique ou de pratique pouvant avoir un impact sur le droit à la vie privée, et à adresser, le cas échéant, un énoncé des incidences à la Chambre des communes.

Le dépôt et la révision (périodique, suite à la révision initiale en fin de cinquième année) de cette nouvelle loi ferait l'objet de vastes consultations publiques.

Le Comité a fait nombre d'autres recommandations, à savoir :

- que soit reconnu, à long terme, un droit constitutionnel explicite à la vie privée;
- que soit adoptée une loi-cadre qui régirait la protection des données détenues par les entreprises privées assujetties à la compétence fédérale;
- qu'il y ait souci d'uniformisation dans l'élaboration des lois sur la vie privée à travers le pays;
- qu'il y ait accès et recours aux technologies facilitant la protection de la vie privée, et appui à la création et à la disponibilité de telles technologies;
- que les citoyens soient davantage sensibilisés aux enjeux liés à la vie privée, et que le Commissariat à la protection de la vie privée du Canada ait un mandat à cet effet.

Le rapport du Comité représente une lueur d'espoir pour le droit, trop souvent batoué, à la vie privée. Ses pages reprennent bien des recommandations que notre Commissariat fait depuis longtemps, et offrent beaucoup de nouvelles idées qu'il peut se sentir à l'aise d'appuyer. Le défi consiste maintenant à traduire par des gestes concrets les préoccupations du Comité. Le gouvernement peut avoir de nouvelles priorités, mais nous tenterons dans toute la mesure du possible qu'il fasse siennes les recommandations du Comité.

Le Comité, dont les travaux ont été échelonnés sur dix mois, a élaboré un plan d'action réfléchi et judicieux qui permettrait au gouvernement de commencer à s'attaquer aux problèmes auxquels font face en cette fin de siècle les Canadiennes et Canadiens en matière de vie privée.

De façon notable, le Comité a souligné l'importance de la vie privée en tant que droit fondamental de la personne. La charte des droits à la protection de la vie privée qu'il propose serait un document « quasi constitutionnel » qui primerait sur toute loi fédérale et garantirait :

- la protection et l'intégrité du corps, de l'esprit et des biens;
- la protection des renseignements personnels;
- l'absence de surveillance;
- la protection des communications personnelles;
- la protection de l'espace personnel.

Ces droits ne pourraient être enfreints que s'il était prouvé qu'il est clairement raisonnable et justifié de le faire dans le contexte d'une société libre et démocratique. En d'autres termes, le respect de la vie privée deviendrait la norme, et ce droit n'aurait pas à être justifié. Il incomberait alors au gouvernement (ou au secteur privé—les banques, par exemple—qui serait assujéti à la compétence fédérale aux termes de la charte proposée) de justifier toute intrusion dans la vie privée.

Le Comité recommande aussi au gouvernement de légiférer afin de « contrer les conséquences possibles des tests génétiques en matière de discrimination et de protection de la vie privée », et de modifier le *Code criminel* en vue d'étendre à la surveillance vidéo l'interdit actuel visant l'interception des communications privées.

Notre Commissariat serait particulièrement touché par quatre recommandations du Comité.

La première vise à remplacer l'actuelle *Loi sur la protection des renseignements personnels* par une *Loi fédérale sur la protection des données*, qui étendrait la protection des renseignements personnels aux fonds de renseignements détenus par le Parlement, tous les ministères et organismes, sociétés de la Couronne, commissions et conseils du gouvernement fédéral, ainsi que par les entreprises privées assujéties à la compétence fédérale (la loi actuelle ne vise qu'environ 105 organismes fédéraux—surtout des ministères—inscrits à son annexe). La nouvelle loi imposerait des règles plus strictes sur le couplage de données au sein du

Jusqu'ou le Parlement doit-il aller?

En avril 1997, peu avant que le Parlement fédéral ne soit dissous en prévision de l'élection fédérale, le Comité permanent de la Chambre des communes sur les droits de la personne et la condition des personnes handicapées déposait un rapport intitulé *La vie privée : où se situe la frontière?* Le Comité, présidé par l'honorable Sheila Finestone, a examiné un certain nombre de questions, en matière de vie privée, soulevées par les nouvelles technologies. Quiconque s'attache à protéger ce qui lui reste de vie privée voudra lire ce rapport.

Mme Finestone s'est inspirée de l'effet de choc qu'ont eu certains rapports du Commissaire à la vie privée du Canada, puis de spécialistes, portant sur les grandes possibilités que recèlent les nouvelles technologies et de leurs conséquences éventuelles sur le droit à la vie privée.

Le Comité a su, à son grand honneur, faire bien plus que certains autres comités parlementaires qui tiennent poliment des audiences publiques, puis remballent sans dire mot. Il a conclu qu'il était grand temps « d'explorer la question de la protection de la vie privée sous l'angle des droits de la personne et d'un point de vue social ». Il s'est vite rendu compte de l'importance de cet objectif : « Au fur et à mesure que nous examinons l'impact des nouvelles technologies sur notre perception de la vie privée, nous nous sommes rendus compte que, finalement, nous étions en train de parler du genre de société que nous entendons édifier pour l'avenir. »

Afin de ne pas crouler sous l'envergure de la tâche, le Comité s'est limité à l'étude de l'impact sur la vie privée de trois technologies, soit la surveillance vidéo, le dépistage génétique et les cartes à puces, en raison de l'imminence et de la pertinence des choix qui s'imposent.

L'examen s'est fait en deux temps. Le Comité a d'abord consulté des spécialistes internationaux en protection de la vie privée (dont bon nombre, peut-on ajouter avec fierté, sont canadiens). Il a ensuite tenu une série de séances publiques à travers le pays pour connaître l'opinion des citoyens à l'égard de la situation en matière de vie privée et le rôle que devrait jouer le gouvernement fédéral pour la protéger.

Il s'agissait là d'un travail démesuré, car si les situations, toujours plus nombreuses, où la technologie menace le droit fondamental à la vie privée submergent de travail le Commissariat, que dire de la tâche qui allait confronter les membres d'un Comité parlementaire, déjà chargés d'autres responsabilités, lors de l'étude de quelques-unes de ces situations seulement?

Il ne faudrait pas non plus prélever de l'ADN si les enquêteurs ne peuvent pas le comparer à des empreintes génétiques liées au crime, tout comme il ne conviendrait pas de le faire si le suspect avoue sa culpabilité. Toutefois, d'un point de vue pratique, la preuve par ADN peut être essentielle, au départ, pour obtenir la déclaration de culpabilité du suspect.

En résumé, voici nos recommandations en ce qui concerne les conditions de prélèvement d'ADN sur des suspects :

- a) le crime doit être violent ou comporter une probabilité de violence;
- b) il doit exister des motifs raisonnables de soupçonner l'individu du crime;
- c) l'échantillon d'ADN doit être pertinent pour prouver l'acte criminel; les enquêteurs doivent pouvoir comparer l'ADN du suspect et l'échantillon lié au crime;
- d) le prélèvement sur le suspect doit être autorisé par un juge.

Notre position apparaissait dans une large mesure dans le projet de loi de 1995 sur les empreintes génétiques. Toutefois, l'Association canadienne des policiers souhaite que trois des quatre mesures de protection de la vie privée soient éliminées : l'exigence qu'il s'agisse d'un crime *violent*; la pertinence du prélèvement pour prouver le délit; et l'obtention d'un mandat d'un juge.

La proposition de l'Association lèverait aussi la restriction, figurant dans le projet de loi de 1995, qu'un prélèvement obtenu par mandat ne soit utilisé que pour faire enquête sur le crime visé.

L'engouement suscité par le concept d'une police toujours plus efficace, doré de technologies intrusives (mais qui pourraient cependant ne pas être la panacée recherchée) ne doit pas l'emporter sur le droit fondamental à la vie privée sans justification claire et impérieuse. L'Association canadienne des policiers n'a pas offert une telle justification.

Nos documents de position sur les deux questions, à savoir la collecte obligatoire d'échantillons d'ADN chez les personnes soupçonnées d'un crime précis, et la création d'une base de données sur les empreintes génétiques, peuvent être obtenus de notre bureau et consultés sur notre site Web, au

<http://infoweb.magi.com/~privcan/>.

Malheureusement, le projet de loi C-94 ne comporte aucune disposition pour assurer que les prélèvements provenant de volontaires et toute l'information qui s'y rattache sont détruits dès que l'innocence du volontaire a été établie.

Rouvrir le débat sur la question de l'ADN sur un autre front
Le 14 avril 1997, peu après le dépôt du projet de loi C-94, l'Association canadienne des policiers a fait paraître des annonces pleine page dans le journal *The Hill Times* demandant que soit étendue les dispositions de la loi actuelle sur l'identification des criminels à la technologie de l'ADN :

Le droit actuel, aux termes de la *Loi sur l'identification des criminels*, autorise la prise d'empreintes digitales au moment de l'arrestation pour un acte criminel; la même chose devrait s'appliquer aux empreintes génétiques puisque la technologie de l'ADN le permet maintenant. [traduction]

L'Association semble favoriser le prélèvement d'empreintes génétiques, à l'instar des empreintes digitales, *de façon tout à fait courante* pour toute personne arrêtée pour un acte criminel. Il est clair qu'elle souhaite s'appuyer sur le projet de loi sur l'identification par les empreintes génétiques pour prélever de l'ADN chez les personnes *soupgonnées* d'un crime—c'est la question qui était au coeur du projet de loi sur les empreintes génétiques, déposé par le Parlement en juin 1995.

La tentative faite par l'Association pour étendre la prise d'empreintes génétiques aux personnes soupçonnées est très troublante. Il est vrai que les empreintes, tant digitales que génétiques, offrent des renseignements permettant d'identifier un individu. Cela s'arrête là pour les empreintes digitales. Toutefois, l'ADN humain est une source considérable d'informations très personnelles qui ne peuvent servir à lier une personne à un crime, mais dont la divulgation peut être très préjudiciable à une personne si elles tombent dans de mauvaises mains.

Le Commissariat a consacré une énergie considérable à assurer que l'ADN puisse être prélevé chez les personnes soupçonnées d'un crime lorsque cela est justifié, tout en respectant les droits légitimes des Canadiens et Canadiennes à la vie privée. Les points que nous avons soulevés dans notre premier mémoire (1995) sur la question de l'analyse génétique à des fins médico-légales sont à réitérer :

La preuve par ADN ne devrait pas être recueillie auprès de suspects de façon systématique, car cela entraînerait une intrusion inutile dans la vie privée. Dans la plupart des affaires criminelles, la preuve par ADN n'apportera rien à l'enquête. Le Parlement ne devrait donc pas donner d'autorisation générale pour que soient prélevés des échantillons d'ADN sur toutes les personnes soupçonnées d'actes criminels.

Nous demeurons fortement opposés à la conservation des prélèvements. L'analyse de l'ADN des substances corporelles suffit pour aider la police à résoudre des crimes, sans qu'il soit nécessaire de conserver les prélèvements.

Les artisans du projet de loi C-94 avaient un choix à faire entre la mesure la moins intrusive, soit conserver l'information nécessaire à l'identification par les empreintes génétiques, et la mesure la plus intrusive, soit conserver les prélèvements eux-mêmes. Ils ont retenu la mesure la plus intrusive.

La gravité de l'envahissement de la vie privée—l'accès par l'État à notre corps—appelle la mesure la moins intrusive. En d'autres termes, on doit se contenter de conserver l'information obtenue seulement. Si cela s'avère une limite incontournable dans les enquêtes, la révision subéquente de la loi permettrait au Parlement de traiter la question. En adoptant la mesure la plus intrusive d'abord, nous ne pourrions déterminer si une intrusion moindre aurait été suffisante. La plupart d'entre nous le savons bien : lorsque l'État obtient un nouveau pouvoir, il s'y accroche.

Nous demeurons préoccupés par la possibilité que les agents de police pourraient être autorisés à prélever des substances corporelles. Le fait qu'un agent de police, et non le personnel médical, effectuerait ce qui constitue fondamentalement un acte médical forcé, qu'il soit mineur ou sans douleur, donne le frisson.

Destruction des prélèvements offerts « spontanément » Le projet de loi ne traite pas d'un autre sujet de préoccupation, soit le traitement des prélèvements provenant de « volontaires ». Un cas d'agression sexuelle récent, à Vermilion, en Alberta, illustre le problème. Au cours d'une enquête, la police a demandé à des résidents d'offrir de leur plein gré un échantillon d'ADN pour l'aider à les soustraire de la liste des hommes soupçonnés du crime (en d'autres termes, de prouver leur innocence, ce qui constitue une distorsion de l'un des tenants fondamentaux de notre système de justice pénale).

Lorsqu'il fournit à la police un prélèvement d'ADN aux fins d'une enquête, un volontaire devrait pouvoir exiger que le prélèvement et toute analyse connexe soient détruits dès qu'il a été établi qu'il n'est pas impliqué dans le crime. Les prélèvements de volontaires ne devraient jamais être conservés, et les analyses effectuées ne devraient jamais être versées dans une base de données. Ils ne devraient pas non plus servir dans des enquêtes sur des crimes autres que celui pour lequel ils ont été sollicités, sauf si la personne y consent de façon éclairée.

- prélever des substances aux fins de dépistage génétique seulement chez les condamnés pour crimes violents, lorsque le risque de récidive est très élevé et qu'on est presque sûr de trouver, sur les lieux du crime, des substances génétiques;
- détruire les échantillons de substances génétiques après obtention de l'information aux fins d'identification; seules les analyses seraient conservées dans les dossiers de la police.

Le projet de loi C-94 proposait une révision générale de la loi cinq ans après son adoption. Toutefois, le traitement de certaines questions était douteux.

« **Infractions désignées** » En premier lieu, la gamme des infractions pour lesquelles des substances pourraient être prélevées chez les condamnés semble inutilement vaste. Il peut paraître dérisoire d'ergoter sur le genre d'infractions criminelles pour lesquelles l'État peut exiger d'un condamné qu'il fournisse une empreinte génétique. Mais c'est loin d'être le cas. Cette technologie permet à l'État de s'introduire dans notre corps même; c'est donc là un pouvoir qui ne devrait être exercé que pour les motifs les plus sérieux. Si l'on jette le filer trop loin, les intrusions dans la vie privée se multiplieront énormément.

Le projet de loi contenait une liste d'« infractions primaires », soit des crimes généralement graves, et fréquemment violents, comme le meurtre, l'agression sexuelle et l'enlèvement. Le prélevement de substances est automatique dans ce cas. Toutefois, une liste d'« infractions secondaires », pour lesquelles la police peut solliciter un mandat de prélevement de substances aux fins d'analyse génétique comprend (entre autres choses) les voies de fait simples, l'introduction par infraction, la destruction d'« autres substances » par le feu, et le défaut d'arrêter lors d'un accident.

Entreposage des prélèvements L'une des réserves les plus graves au sujet du projet de loi C-94 vise le projet d'entreposer les *prélèvements* eux-mêmes, plutôt que les seules *analyses* ayant servi à obtenir l'information nécessaire. Aux termes de la loi, l'empreinte génétique servirait à lier l'auteur d'une infraction à un crime précis. Le fait de conserver les prélèvements eux-mêmes aboutira inévitablement à d'autres utilisations ayant peu à voir avec l'identification des criminels; par exemple, permettre aux chercheurs d'utiliser les prélèvements pour étudier le lien entre le profil génétique et le comportement criminel. Notre siècle a déjà été témoin d'une utilisation à mauvais escient de la recherche génétique appliquée au comportement criminel (la théorie du chromosome XYY, qui était censée permettre d'identifier les hommes violents).

Le 10 avril 1997, le gouvernement a déposé devant le Parlement le projet de loi C-94, *Loi sur l'identification par les empreintes génétiques*. La loi a pour objet l'établissement d'une banque de données génétiques à partir de prélèvements de substances corporelles provenant de condamnés pour aider la police à identifier les auteurs de crimes non résolus. Il constitue la deuxième phase du plan du gouvernement pur régler l'analyse génétique comme outil d'identification des auteurs de certains crimes. Il est demeuré en plan au feuilleton en raison de l'élection. Plusieurs aspects sont cause d'inquiétude, mais nous avons maintenant la possibilité de redresser la situation.

Retournons d'abord en arrière. La première phase du plan du gouvernement à l'égard du dépistage par les empreintes génétiques a été adoptée en 1995; elle permettrait à la police de recueillir des échantillons d'ADN sans le consentement des auteurs présumés d'infractions criminelles, en général des personnes impliquées dans un crime avec violence. L'échantillon prélevé était destiné à être comparé aux substances trouvées sur le lieu d'un crime pour déterminer si une personne soupçonnée d'avoir commis le crime l'aurait réellement commis. Le projet de loi ne traitait pas de la conservation de l'information obtenue ou de l'entreposage des substances prélevées. Cela constituait l'une des nombreuses questions dont l'étude a été reportée à la deuxième phase.

Nous avons appuyé avec circonspection le projet de loi de 1995. La preuve basée sur les empreintes génétiques peut aider à obtenir un verdict de culpabilité ou d'innocence, et le projet de loi de 1995 fournissait un mécanisme raisonnable pour assurer que des substances aux fins d'identification génétique n'étaient pas prélevées inutilement chez les auteurs présumés d'infractions. Puis, au début de 1996, le Solliciteur général a diffusé un document de travail (Une banque nationale de données génétiques) qui traitait de plusieurs autres questions, y compris la conservation, et sollicitaient les commentaires des personnes intéressées.

Nous avons offert en réponse au gouvernement plusieurs suggestions à étudier avant le dépôt du projet de loi. Nous avons notamment suggéré que trois conditions importantes doivent être satisfaites pour répondre aux préoccupations en matière de protection de la vie privée :

- réviser la loi trois à cinq ans après son adoption; on ferait entre autres une mesure l'intrusion suscitée par la création de la base de données était justifiée par la résolution d'un nombre plus grand de crimes violents grâce aux empreintes génétiques;

accusateur est un principe fondamental de la vie privée et de la justice naturelle. On ne doit y déroger que dans des cas exceptionnels. La mise en place d'un cadre exhaustif de protection des renseignements personnels renforcerait l'exactitude et le caractère courant des renseignements en permettant au requérant de faire corriger les erreurs de fait et de signaler les renseignements contestés. En outre, on devrait tenter de mieux cerner quels types de renseignements personnels « additionnels » sont pertinents à l'octroi d'un permis afin d'éviter la collecte de renseignements à l'aveuglette.

La seconde lacune concerne un processus de révision provisoire à l'intention des personnes dont la demande de permis a été rejetée. À l'heure actuelle, le seul recours qui s'offre au requérant est de s'adresser directement à la cour. En sus du fardeau que cela impose au requérant, sans parler des tribunaux, cela risque de mener à la communication publique de renseignements de nature potentiellement délicate, dont certains peuvent être contestés. Cette démarche de contestation d'une décision administrative paraît plutôt lourde, alors qu'une tierce partie indépendante ou encore une commission ferait autant l'affaire, et à moindre coût.

Le Sous-comité a adopté le règlement, mais il a fait deux recommandations concernant la protection des renseignements personnels. Dans un premier temps, il a préconisé que le gouvernement négocie une entente avec chaque province et territoire à l'effet que la *Loi sur les armes à feu* est une loi fédérale, assujettie à la *Loi sur la protection des renseignements personnels* là où il n'existe pas de loi semblable au palier provincial, et précisant les règles d'application dans ces administrations. Le gouvernement a accepté la recommandation.

Toutefois, le gouvernement a rejeté la seconde recommandation, portant sur un mécanisme de médiation permettant au requérant de contester des renseignements soi-disant faux ou inexacts sans devoir s'adresser à la cour. Il a soutenu que les techniques d'enquête permettent déjà d'assurer que les décisions ne sont pas basées sur des renseignements inexacts et que les enquêtes permettront normalement au requérant de se faire entendre. Tout en étudiant comment le processus d'enquête pourrait être amélioré en tenant compte des préoccupations en matière de protection des renseignements personnels, le ministère de la Justice a rejeté la médiation en la jugeant incompatible avec les objectifs de sécurité dérogatoires stipulés dans la loi.

Le Commissaire demeure sceptique.

renseignements médicaux et familiaux très personnels lorsqu'une demande d'acquisition d'une arme à feu sera présentée. Le Commissaire a donc conseillé que le code de pratiques équitables du traitement de l'information de la *Loi sur la protection des renseignements personnels* serve de modèle pour la collecte, l'utilisation et la communication de tous les renseignements personnels consignés au registre et il a recommandé que ces principes soient clairement inscrits dans la loi.

En avril 1996, le premier règlement a été soumis; il a par la suite été retiré, puis en novembre, une nouvelle version, très peu détaillée, a été présentée. Néanmoins, le résumé de l'étude d'impact de la réglementation précisait clairement que les « questions d'accès à l'information et de protection des renseignements personnels sont prévues par la législation fédérale et provinciale pertinente » et que « la loi à cet égard est très vaste et régira adéquatement les questions... ».

Le Commissaire ne partageait pas cet avis. En février 1997, lorsqu'il a paru devant le Sous-comité de la Chambre des communes étudiant le règlement, il a d'abord rappelé que ce ne sont pas toutes les administrations qui disposent d'une loi sur la protection des renseignements personnels. Deuxièmement, certaines lois provinciales traitent uniquement de l'accès d'une personne à ses renseignements personnels et ne régissent aucunement la collecte, l'utilisation et la communication des renseignements personnels. Enfin, certaines lois provinciales ne s'appliquent pas aux forces policières municipales, qui sont fréquemment les organismes chargés de recueillir et de contrôler ces renseignements. Bref, la protection juridique comporte de grosses lacunes.

Puisque les règlements en soi sont très succincts, il semble que seules la structure et l'esquisse du processus fourniront des réponses après coup—beaucoup trop tard pour offrir une protection juridique. Cependant, deux règlements méritent qu'on s'y attarde. Le premier a trait à la méthode d'obtention d'un permis d'armes à feu, aux termes de laquelle la police doit signaler la demande de permis aux conjoints, actuels et anciens, du requérant; il comporte de vastes pouvoirs discrétionnaires pour la collecte de renseignements « additionnels » au sujet des requérants.

L'objet des règlements est clairement d'assurer la protection du public, collectivement et individuellement, mais le processus doit faire obligation aux organismes recueillant ces renseignements pour que ces derniers soient crédibles et pertinents. Toute personne fournissant des renseignements qui serviront à établir si un requérant devrait se voir accorder un permis doit être disposée à ce que ses commentaires soient transmis au requérant. Le fait de pouvoir confronter son

Le registre des armes à feu

K1A 0M6.

Toute personne qui a été mal informée et souhaite que son nom ne figure pas sur la liste électorale permanente peut obtenir que son nom soit retiré en faisant la demande par écrit au Directeur général des élections, 257, rue Slater, Ottawa,

Les questions de protection des renseignements personnels que suscite le projet de loi sur le contrôle des armes à feu étaient manifestes en 1994 lorsque le gouvernement a fait part de son intention de constituer un tel registre. Le personnel du Commissariat a rencontré les représentants du Bureau d'enregistrement des armes à feu pour discuter du genre de renseignements qui seraient recueillis, qui en feraient la collecte, où et sous le contrôle de qui ces renseignements seraient conservés; et par là même, à quelles lois sur la protection des renseignements personnels ils seraient assujettis. La gestion des renseignements était une question importante car le modèle envisagé ressemblait quelque peu à celui du Centre canadien d'information de la police (CCIP), qui est un système de données géré par la Gendarmerie royale du Canada, mais qui ne relève pas du gouvernement fédéral et qui n'est donc assujetti qu'en partie à la loi fédérale sur la protection des renseignements personnels. Son statut a soulevé d'épineuses questions de compétence pour plus d'un commissaire à la vie privée. (Le CCIP est maintenant doté d'un code national de protection des renseignements personnels que tous les membres doivent respecter).

La *Loi sur les armes à feu* (loi C-68) a été adoptée par le Parlement en juin 1995 sans qu'il n'y soit fait mention à la protection des renseignements personnels et sans que le registre ne soit assujéti, en raison de son caractère hybride, à la loi fédérale sur la protection des renseignements personnels. Le Commissaire a reçu l'assurance que les dispositions en matière de protection des renseignements personnels seraient clairement stipulées dans les règlements qui seraient adoptés par la suite et qu'il serait invité à offrir ses observations à ce moment. Le Comité sénatorial permanent des affaires juridiques et constitutionnelles, qui était conscient des questions de protection des renseignements personnels en jeu, a demandé au Commissaire de comparative.

En bref, le Commissaire a fait remarquer que la loi prévoyait la collecte de renseignements personnels importants et de nature potentiellement délicate, qui devaient être protégés par la loi ou, à défaut, par les règlements. Les contrôleurs d'armes à feu conserveront les dossiers de chaque permis et certificat émis et révoqué, des demandes rejetées, des cas d'armes perdues, trouvées, volées ou détruites, et des importations et exportations d'armes. En outre, les contrôleurs locaux, qu'ils soient provinciaux ou municipaux, auront à recueillir des

communiquées aux partis politiques et aux candidats, car il a soutenu que la communication de ce renseignement ferait du processus électoral un moyen de sollicitation par téléphone des votes. Bien entendu, les partis politiques peuvent acheter le logiciel permettant de coupler la liste électorale aux boîtiers téléphoniques électroniques, mais ils le font à leurs propres frais. Elections Canada a retiré le numéro de téléphone du nombre de renseignements à obtenir pour les élections (des provinces exigent ce numéro pour les élections provinciales).

Pouvoir de recueillir d'autres renseignements mieux défini

Le pouvoir illimité dont jouissait le Directeur général des élections pour recueillir des renseignements personnels est maintenant plus étroitement défini, car il se fait sur entente avec les provinces. Elections Canada sera donc autorisée à obtenir des renseignements additionnels (telle que la profession) s'ils sont exigés pour voter dans une province. D'autres renseignements ne figureront pas sur la liste compilée en vue d'une élection fédérale.

Droit à ne pas figurer sur la liste En termes de protection des renseignements personnels, la question la plus fondamentale concernait le droit à ne pas figurer sur la liste électorale permanente, et Elections Canada ne s'y est pas opposé. Une personne pourra ne pas être inscrite sur la liste sans être privée de son droit de vote, mais elle devra faire la démarche nécessaire pour que son nom soit ajouté à la liste lorsqu'une élection est déclenchée.

Malheureusement, en dépit des meilleures intentions, cet aspect du nouveau processus pourrait avoir échoué. D'après des observations, de l'aveu de tous informelles, du personnel et des personnes qui ont communiqué avec les divers commissaires, il semble que les recenseurs auraient mal compris le caractère optionnel de la liste. En fait, certains ont déclaré à des Canadiens que, si leur nom ne figurait pas sur la liste, ils ne pourraient pas voter. Toutefois, les recenseurs ne sont pas en faute; il se peut que le caractère optionnel de l'inscription sur la liste ne leur ait pas été signalé. Le personnel de protection des renseignements personnels a confirmé que la trousse de formation ne mentionnait pas cette option; il semblerait que le sujet devait être traité de vive voix durant la séance de formation des recenseurs, d'une durée de deux heures.

On conviendra que le fait de former 96 000 recenseurs à travers le pays constitue un défi de taille en matière de communication, et on peut excuser les lacunes relevées. Compte tenu de l'intérêt et de l'engagement manifesté par le Directeur général des élections et de son personnel à l'égard de la protection des renseignements personnels figurant sur la liste électorale, nous espérons que ces problèmes seront corrigés.

Autres utilisations de la liste La principale préoccupation suscitée par la liste est que le gouvernement pourrait être tenté d'en faire des utilisations secondaires. Soumis à des pressions budgétaires croissantes et dotés de moyens électroniques, les bureaucrates se sentent de plus en plus les coudes franches pour utiliser à d'autres fins les renseignements personnels—d'après le raisonnement suivant : « Pourquoi vous inquiétez-vous si vous n'avez rien à cacher? ». Le Commissaire a donc cherché à obtenir des garanties législatives que la liste permanente ne servirait pas à des fins autres que la tenue des élections. La Loi interdit maintenant toutes autres utilisations.

Mise à jour par couplage des données Une deuxième réserve importante concernait le projet de mettre à jour la liste électorale en allant extraire des renseignements personnels d'autres bases de données fédérales, comme celle des déclarations d'impôt. Ce genre de couplage de données est invisible et enfreint un principe fondamental de protection de la vie privée, soit celui du consentement éclairé.

À la recommandation du Commissaire, Elections Canada a accepté que le couplage de données n'ait lieu que si l'électeur y consent. L'an prochain, le formulaire de déclaration d'impôt comportera une case offrant à l'électeur l'option d'accepter que Revenu Canada transfère à Elections Canada des renseignements strictement courants (nom, adresse et date de naissance). Revenu Canada ne communiquera aucun autre renseignement. En outre, les nouveaux citoyens pourront demander que Citoyenneté et Immigration Canada expédie les renseignements pertinents à Elections Canada aux fins de la liste électorale permanente. Le couplage de données avec une base de données provinciale (permis de conduire, liste électorale provinciale ou municipale, etc.) devra se faire conformément aux lois provinciales sur la protection des renseignements personnels.

Communication annuelle de la liste électorale aux partis politiques

Avant la récente série d'amendements, les partis politiques et les candidats recevaient copie de la liste seulement lorsque des décrets de convocation des électeurs étaient délivrés. Les amendements adoptés autorisent la communication annuelle de la liste à tous les partis qui ont un candidat dans une circonscription, ainsi qu'au député actuel, car on suppose qu'elle sera mise à jour plus ou moins régulièrement. Le Commissaire juge que cette communication annuelle est excessive, qu'elle est inutile pour le processus électoral et qu'elle pourrait inciter à une sollicitation des votes plus fréquente. Néanmoins, le Parlement l'a approuvée.

Pas de collecte de numéros de téléphone Le Commissaire s'est aussi opposé à la collecte des numéros de téléphone et à leur inclusion dans les listes

En matière de registres de la population, un défi perpétuel se pose à l'ombudsman de la vie privée, à savoir où s'établit la distinction entre l'acceptation pragmatique des listes dressées à des fins administratives (avec protection solide des renseignements personnels) et un sentiment d'inquiétude salubre face aux pressions croissantes pour l'identification et la quantification des citoyens dans diverses bases de données. Lorsqu'un nom est versé dans une base de données, il n'y a qu'un pas à franchir, au nom d'une plus grande efficacité, vers l'établissement d'un profil exhaustif.

Cette année, le Commissariat a suivi la création de plusieurs registres avec plus ou moins d'inquiétude : la liste électorale permanente, le registre des armes à feu et la banque de données projetée de l'ADN.

La liste électorale permanente

Le 10 avril 1997, les recenseurs fédéraux sont passés pour la dernière fois de maison en maison pour faire le recensement. Les renseignements recueillis serviront à élaborer la liste électorale permanente, qui est la point culminant de plusieurs années de travail à Elections Canada. Dès maintenant, la liste électorale pour les élections fédérales et, peut-être, provinciales et municipales, sera mise à jour à partir d'autres bases de données fédérales (avec le consentement de l'électeur) et, éventuellement, de banques de données provinciales désignées.

Elections Canada envisageait depuis longtemps de dresser une liste électorale permanente, mais ce n'est qu'en 1994 que le travail a été entrepris sérieusement. Au fait des inquiétudes du Commissaire au sujet de l'élaboration d'une telle liste, Elections Canada lui a demandé sa collaboration systématique durant le déroulement du projet. Le Commissaire a accepté et a offert les services d'un des employés. Il a mis l'accent durant l'exercice sur le genre de renseignements que les Canadiens devaient consentir pour exercer leur droit de vote et sur la meilleure façon de protéger les renseignements versés dans une base de données électronique.

Des amendements à la *Loi électorale du Canada* ont été déposés en octobre 1996 à la Chambre des communes, et on a demandé au Commissaire de comparer pour offrir ses observations sur les effets qu'ils auraient en matière de protection des renseignements personnels. Les amendements reprenaient la plupart des recommandations du Commissaire figurant dans son rapport annuel de 1995-1996 à la rubrique « Voter librement » (page 15).

Le rapport final du Forum national sur la santé fait état de l'importance de respecter la vie privée lors de l'élaboration d'un réseau national d'information sur la santé. Le ministère fédéral de la Santé compte traiter de cet enjeu crucial dès la planification du réseau, et nous nous proposons de l'aider. Selon le respect qu'il a de notre vie privée, de notre autonomie individuelle et de la valeur de notre consentement, le réseau canadien d'information sur la santé qu'envisage le Forum peut devenir tout aussi bien un franc succès qu'un désastre. L'importance qu'un tel réseau accordera à notre vie privée déterminera notre acceptation ou, selon le cas, la véhémence de notre refus devant l'incroyable surveillance dont nous pourrions être l'objet.

Il nous tarde d'avoir sous les yeux les dispositions juridiques qui garantiront la confidentialité de nos renseignements médicaux.

Erratum : Le rapport annuel de l'année dernière faisait référence au manque de protection juridique des données nationales d'un sondage menée par l'Institut canadien de l'information sur la santé. En fait, ce sondage est mené par Statistique Canada sous l'autorité et (sous la protection) de la *Loi sur les statistiques*. Nous regrettons l'erreur.

- la sensibilisation des patients aux usages qui sont faits de leurs dossiers médicaux, ainsi qu'aux conséquences pour leur vie privée de l'informatisation et de l'inclusion de ces dossiers dans un réseau national;
 - la rédaction de lignes directrices qui traiteront des enjeux de l'informatisation de dossiers médicaux, pour la vie privée des patients et la sécurité des dossiers médicaux. Ces lignes directrices comporteraient notamment de modalités de contrôle et de vérification;
 - la mise en place d'un mécanisme indépendant permettant de s'assurer que soient respectées la vie privée et la confidentialité des renseignements de nature médicale.
- Le lien des dossiers médicaux à des bases de données sur l'emploi, l'éducation et autres facteurs socio-économiques révélerait bien plus que des renseignements médicaux, car la vie de chaque citoyen deviendrait un livre ouvert. Cela semble être l'objectif visé par le secteur de la santé. Il paraît facile de justifier les bénéfices que tous en retireraient, mais il ne faut pas oublier que ces renseignements pourraient servir à des fins préjudiciables : bien que servant à l'origine à la prestation de soins de santé, la collecte de renseignements sur la santé pourrait insidieusement mener à une surveillance médicale, à une surveillance de notre style de vie et, en fin de compte, à la surveillance généralisée par l'État.
- Il est donc extrêmement important de voir comment éviter tout usage secondaire de nos renseignements médicaux par les forces de l'ordre, les employeurs ou des particuliers trop curieux (pratiques répandues aux États-Unis). Les bases de données médicales ne doivent servir qu'à l'amélioration des soins de santé et rien d'autre. Elles ne doivent jamais devenir un outil pratique dont se serviraient gouvernements et entreprises privées pour surveiller, à des fins autres que médicales, un citoyen se prévalant simplement d'un service essentiel.
- Il faut évidemment atteindre un équilibre entre les deux pôles que sont une meilleure santé publique et personnelle et notre autonomie individuelle. Nous reconnaissons les usages bénéfiques qui peuvent être faits des renseignements médicaux, ainsi que l'importance de la recherche. Mais il existe une différence de taille entre l'usage de renseignements personnels reliés à un individu identifiable, et le recours à des données collectives anonymes. Dans l'intérêt du maintien de l'honnêteté et de la confiance entre un patient et son médecin, nous insistons sur l'importance de protéger la vie privée des citoyens et la confidentialité de leurs renseignements médicaux. La protection de la vie privée est aussi prioritaire que l'amélioration du régime de soins de santé.

intérêt public. Les données médicales deviendraient un produit privilégié sur le marché des renseignements.

Avant de se précipiter vers le paradis que représente pour certains un régime de soins de santé fondé sur les résultats cliniques, le Canada devrait réfléchir très sérieusement aux dangers qu'une telle concentration de renseignements personnels, d'ordre médical ou autres, ferait courir à notre vie privée et à notre autonomie individuelle.

Certaines personnes peuvent ne pas s'élever contre la diminution de la confidentialité de leurs dossiers médicaux. Toutefois, la liberté de choisir de participer à un plan aux incidences si vastes est un élément essentiel de la protection de la vie privée et de la démocratie, et doit être préservée. Afin de protéger les droits de ceux qui s'opposeraient à un tel plan, tout réseau de santé informatisé doit permettre aux particuliers d'empêcher que leur dossier médical ne soit versé dans le réseau. En outre, on ne devrait pas pénaliser une personne qui choisit de ne pas voir son dossier médical versé dans le réseau en lui accordant des soins de santé de moindre qualité.

Il est primordial de cerner les questions qui touchent à la préservation de la protection des renseignements de santé. Voici ce que nous suggérons :

- L'adoption de lois fédérales et provinciales complémentaires garantissant la confidentialité de l'ensemble des renseignements médicaux reliés à un individu identifiable. Ces lois incorporeraient les principes de gestion équitable de l'information qui figurent dans les accords internationaux en matière de protection des données, et elles devraient précéder l'élaboration du réseau proposé par le Forum;
- L'établissement de paramètres clairs entourant le consentement d'un patient à la communication de son dossier médical. En cas de refus, le droit du patient de contrôler la diffusion de ses renseignements primerait sur toute autre raison, sauf un intérêt public généralisé et contraignant (ou afin de dispenser des soins d'urgence au patient). Les recherches scientifiques menées ne se situent pas toujours dans le cadre de l'intérêt public.
- L'établissement de limites strictes relativement aux situations où l'accès à des renseignements personnels est permis pour des activités secondaires telles que la recherche, et l'encouragement à utiliser des données collectives anonymes pour la recherche;
- L'instauration de puissants recours juridiques en cas de communication non autorisée de renseignements médicaux;

et une circulation accrues de renseignements médicaux ne peuvent qu'alarmer au chapitre de la vie privée.

La protection de la vie privée dans un contexte médical signifie généralement que seules les personnes intervenant directement dans la prestation des soins ont accès aux dossiers médicaux des patients. Les strictes normes éthiques et les lois régissant la profession assurent que les dossiers font l'objet de précautions et d'une confidentialité des plus élevées. À peu d'exceptions près, le patient dispose seul du plein contrôle de ses renseignements médicaux, lequel ne relève donc pas de son docteur, de l'hôpital ni de l'État.

Le recours à un réseau informatisé à l'appui de soins de santé fondés sur les résultats cliniques constitue un revirement total par rapport à cette règle centenaire. Alors qu'aujourd'hui seuls le patient et quelques autres personnes ont le droit de consulter le dossier médical du patient, demain ce dossier ne serait plus confidentiel puisqu'il pourrait être consulté électroniquement par des centaines d'inconnus.

La situation qui prévaut aux États-Unis est digne d'intérêt. Rappelant cette remarque parue dans une revue médicale à l'effet que la pratique médicale est de plus en plus un sport de spectateurs, les juristes américains Paul Schwartz et Joel Reidenberg expliquent "qu'un nombre croissant d'observateurs étudient la performance des médecins, du personnel infirmier et des patients, et que les renseignements personnels jouent un rôle essentiel à l'évaluation de leur comportement". [Traduction]

Certains diront que la situation canadienne est différente, que nos renseignements personnels sont mieux protégés parce que notre régime de santé est fortement contrôlé par l'État. C'est justement à cause du rôle étendu de l'État dans la prestation des soins de la santé qu'il est important qu'il y ait des mécanismes en place pour rétablir l'équilibre et exercer un certain contrôle. Même si les Canadiens perçoivent l'intervention de l'État comme peu menaçante, il ne faut pas abdiquer notre responsabilité individuels.

Par ailleurs, notre régime se privatise de plus en plus; ainsi, des firmes privées dispensent actuellement les soins à domicile, les services de phoniatre ainsi que divers types de tests. Avec l'arrivée des régimes pour les médicaments, les pharmaciens (qui ont toujours appartenu au secteur privé) transigent fréquemment avec les compagnies d'assurance privées, et le tout de plus en plus par voie électronique. À l'instar de nos voisins du sud, nos renseignements pourraient être de plus en plus utilisés à des fins autres que cliniques et ne satisferaient à aucun

et le niveau de scolarisation des patients. Ils souhaitent de plus que les chercheurs du domaine de la santé soient exemptés des dispositions habituellement contenues dans les lois protégeant la vie privée, soit l'obtention du consentement des individus à l'usage de leurs renseignements pour des fins de recherche ou d'autres communications, et la destruction de ces renseignements à une date donnée.

En bref, le rapport du Forum pousse les gouvernements à consommer davantage de renseignements médicaux au nom d'un plus grand contrôle et d'une meilleure gestion des services de soins de santé. Il prône également l'accès par les chercheurs aux renseignements sur tous les habitants du pays, tout en exemptant ces mêmes chercheurs des obligations que les lois canadiennes sur la protection de la vie privée leur imposeraient normalement en matière d'accès et d'utilisation de tels renseignements. Enfin, l'efficacité des soins et de la recherche exige, semble-t-il, que l'ensemble de ces renseignements soit informatisé afin d'en faciliter l'échange entre toutes les parties intéressées.

Il nous est impossible de savoir si une médecine fondée sur les résultats cliniques serait de qualité supérieure. Cependant, l'adoption d'un réseau informatique usant de telles données représente peut-être l'un des enjeux les plus importants de ces dernières années pour la vie privée des Canadiennes et Canadiens. Un tel réseau révolutionnerait en effet la collecte, la communication et l'usage de données, exigeant l'intégration, au moyen de technologies informatiques de pointe, de quantité de renseignements : données médicales provenant de docteurs, d'hôpitaux et de pharmacies, et renseignements socio-économiques (éducation, revenu, etc.). Les utilisateurs de toutes ces données ne seraient plus seulement les professionnels de la santé, mais également tous les administrateurs et autres décideurs qui s'en serviraient pour orienter les soins. L'accès, non pas à des données collectives anonymes, mais à des renseignements spécifiques au sujet d'un tel individu identifiable, constitue l'un des éléments clés du développement d'un tel système.

Il est difficile de s'opposer à un projet qui permettrait d'arriver à des décisions mieux éclairées; après tout, les défenseurs de la vie privée veulent de bons soins de santé tout autant que le reste de la population canadienne. Nous comprenons également qu'une recherche clarifiée pourrait permettre de mieux comprendre les facteurs influant sur la santé et d'améliorer la prestation des soins de santé. Mais l'utilisation de renseignements médicaux en vue d'améliorer le régime canadien de soins de santé ne comporte pas que de bons éléments. En effet, les recommandations du Forum menacent sérieusement la confidentialité des dossiers médicaux de tous les habitants de notre pays, ainsi que les droits de ces derniers de connaître, d'approuver et de contrôler les usages qui en sont faits. Une collecte

Un dossier médical électronique... et national!

En octobre 1994, le premier ministre du Canada mettrait sur pied un groupe de spécialistes afin de faire participer et d'informer la population quant aux enjeux reliés au secteur de la santé. Ce Forum national sur la santé devait de plus conseiller le gouvernement fédéral sur les façons d'améliorer la santé des citoyens et le régime de soins de santé. Le rapport final du Forum, déposé en février 1997 et intitulé *La santé au Canada : un héritage à faire fructifier*, recommandait notamment que l'amélioration des décisions en matière de santé passe par l'utilisation de meilleurs renseignements ou de résultats cliniques pertinents, équilibrés et de meilleure qualité. Il s'agit là, dans le jargon de la profession, de médecine fondée sur l'expérience clinique.

Les membres du Forum ont plus particulièrement suggéré de se pencher sur le rôle que les technologies de l'information peuvent jouer dans la mise sur pied d'un réseau national d'information sur la santé. Dans son budget de 1997, le gouvernement fédéral a d'ailleurs prévu un montant de 50 millions de dollars pour l'élaboration d'un réseau national de suivi médical, d'une base nationale de dossiers médicaux et d'un réseau médical pour les autochtones.

Les membres du Forum suggèrent aussi que les organismes provinciaux et territoriaux établissent un ensemble normalisé de données médicales longitudinales pour suivre l'évolution de la santé d'un particulier sur une longue période.

Le rapport du Forum indique enfin qu'il ne suffit pas de rassembler et d'intégrer tous les renseignements médicaux sur les citoyens, car l'état de santé d'une personne subit en effet l'influence d'un certain nombre de facteurs, dont plusieurs ne sont pas de nature médicale. Les membres du Forum s'intéressent donc aux liens entre la santé et le statut social, soit l'effet de facteurs socio-économiques tels la pauvreté, le chômage et les réductions d'aide sociale sur la santé d'une personne.

Croyant que l'usage de telles données par des chercheurs serait bénéfique pour la société, le rapport des membres du Forum préconise un lien informatique entre les données cliniques et administratives et d'autres renseignements de nature non médicale portant sur le revenu, l'emploi et l'éducation des citoyens.

Les membres du Forum recommandent donc de relier les données médicales de nature clinique et administrative aux renseignements décrivant le revenu, l'emploi

indépendance pour pouvoir mener enquête, de façon crédible et impartiale, sur les plaintes.

Le commissaire fédéral à la vie privée n'est pas la seule personne que cette question préoccupe. Les commissaires provinciaux et territoriaux suivent le projet avec circonspection. Le Commissariat a consenti à recueillir et à échanger l'information, ainsi qu'à coordonner la réponse des commissaires à la vie privée.

vie privé constitue l'obstacle le plus fort à la mise au point d'un code d'identification commun.

À cet égard, le rapport est dans le vrai. Il est noble de vouloir fournir de façon plus efficace les services gouvernementaux, mais ce faisant il se pourrait que nous démolissions les murs soigneusement construits qui protègent nos dossiers de données personnelles. Ces murs empêchent les gouvernements d'établir des profils personnels complets de leurs citoyens et d'utiliser les renseignements recueillis à une fin précise pour une autre fin, totalement sans rapport avec la première. Dans ce contexte, la protection des renseignements personnels exige, comme l'énonce une décision de la Cour suprême des États-Unis, « que nous protégeons les valeurs fragiles de nos citoyens vulnérables face à la préoccupation arrogante à l'égard de l'efficacité qui peut caractériser les fonctionnaires dignes d'éloge tout autant, voire davantage, que les fonctionnaires médiocres ». [Traduction]

Le gouvernement doit examiner attentivement plusieurs questions avant d'accepter le concept d'un code d'identification commun. En premier lieu, la poursuite de la création d'un tel code doit reposer sur des motifs sérieux et avérés. À ce jour, aucune preuve empirique n'est venue appuyer un tel concept. Ce n'est pas l'enthousiasme à trouver une solution rapide aux problèmes sociaux et économiques en s'appuyant sur la technologie qui fait défaut, mais l'espoir que de tels solutions ne remplaceront pas une analyse stricte du bien-fondé véritable du recours à une telle technologie.

En deuxième lieu, si on devait conclure qu'un code d'identification commun répond de façon manifeste à un besoin, une loi devrait être adoptée avant que cette création n'ait lieu. Comme l'a fait remarquer le commissaire à la vie privée de l'Alberta, Robert Clark, les « technocrates » ne doivent pas empiéter sur les « démocrates ». Les utilisations des mécanismes d'identification et de protection des renseignements personnels doivent être énoncées clairement dans la loi, et toute utilisation abusive du système doit être punie sévèrement.

En dernier lieu, l'impact de l'introduction d'un code d'identification commun doit être pleinement compris avant la mise en oeuvre d'un tel code. L'impact sur la vie privée et l'impact sur la société en général doivent être évalués. Même si le rapport n'a pas reçu de sanction officielle, le ministère du Développement des ressources humaines s'en servira probablement pour analyser la rentabilité d'un code d'identification commun dans les programmes de sécurité du revenu.

La Commissaire à la vie privée a consenti à fournir des commentaires sur l'impact considérable du projet sur la vie privée, accompagnés de la mise en garde habituelle; il n'est pas autorisé à juger de la qualité du projet. Il doit préserver son

Le rapport relève plusieurs éléments importants d'un code d'identification commun efficace, entre autres, le besoin de l'étendre à toutes les administrations et d'être unique à l'individu, l'applicabilité à tous les programmes de prestation, et la sécurité à l'égard de la reproduction ou de l'altération frauduleuses. Le code d'identification commun doit aussi assurer la protection des renseignements personnels et aboutir à un minimum d'intrusion dans la vie privée des clients. Le groupe a envisagé diverses options :

- le statu quo (nom, date de naissance)
- le numéro d'assurance sociale actuel (NAS)
- un NAS « modernisé » (exigeant l'identification positive du client par l'obligation d'entrer un numéro d'identification personnel) et l'établissement d'un registre des NAS comme base de données centrale dans laquelle seraient versés les noms des prestataires de tous les programmes de sécurité du revenu
- un « nouveau » numéro servant de code d'identification commun pour les programmes de sécurité du revenu de tous les paliers de gouvernement
- le numéro de l'assurance-santé provinciale.

Le groupe semble privilégier un NAS modernisé (le NAS actuel servant de code d'identification provisoire) ou un nouveau numéro spécialement créé. L'option d'utiliser le numéro de l'assurance-santé ou une carte « biométrique » semble avoir été rejetée pour le moment.

Nous sommes disposés à être réceptifs à être reçus de nombreux aspects du travail du groupe, mais toute proposition fondée sur le NAS actuel recèle des difficultés. Ce code d'identification personnelle est fortement galvaudé. Bien que le gouvernement fédéral ait adopté, depuis 1989, une politique limitant les utilisations qu'il en fait, le NAS se retrouve partout. Les propriétaires, les agences d'évaluation du crédit, les bibliothèques, les clubs vidéo, les supermarchés s'en servent, la liste de ceux qui ne l'utilisent pas est nettement moins longue à dresser que la liste des utilisateurs. Il serait précaire de baser le code d'identification commun sur le NAS.

Le groupe de travail admet qu'on compte au nombre des obstacles à la création d'un code d'identification commun les préoccupations des particuliers au sujet de la confidentialité et de la protection de leurs renseignements personnels; les restrictions à imposer à l'égard du partage et de la communication de ces renseignements dans les programmes de sécurité du revenu et les dispositions juridiques à prendre en matière de la vie privée; et les restrictions juridiques quant à l'utilisation du NAS. En fait, le rapport précise que l'impact perçu sur la

Service tout en un : le code d'identification commun

L'année dernière, tous les paliers de gouvernement ont étudié de nouvelles façons d'améliorer l'exécution des programmes de sécurité du revenu et de mettre en commun les renseignements personnels de leur clientèle. Ils sont d'avis, non sans raison, que les Canadiens n'ont pas de préférence quant au palier de gouvernement qui fournit un service aussi longtemps que ce service est fourni.

Toutefois, l'impact immédiat de la mise en commun, par les différents gouvernements et organismes, des renseignements personnels et l'exécution concertée des programmes est que ces renseignements deviendront plus largement accessibles au sein des gouvernements et entre eux. Ces renseignements seront reliés et mis en commun par nombre d'utilisateurs, les particuliers auront encore moins de contrôle sur leurs renseignements personnels. En outre, en raison de cette accessibilité plus grande, ces renseignements personnels seront presque inévitablement plus vulnérables à une utilisation ou un échange autres que les fins d'origine.

Une deuxième préoccupation concerne le besoin d'une méthode commune à tous les paliers de gouvernement pour identifier le client. Les gouvernements souhaitent donc mettre au point un « code d'identification commun », parce ce qu'une identification fiable du client est requise à toutes les étapes du processus de demande et de paiement des prestations, d'établissement de liens avec d'autres programmes et services, de tenue des dossiers, de lutte contre la fraude et l'erreur, et de cessation des prestations. Un code d'identification commun est donc jugé essentiel, tout autant qu'une base de données centrale, accessible à tous les programmes de sécurité du revenu et à tous les paliers de gouvernement.

En fait, les propositions se traduisent par un couplage des données systématique et complet, à une échelle tout à fait inédite.

Un groupe de travail composé de gestionnaires de la technologie de l'information des ministères de sécurité du revenu des gouvernements fédéral, provinciaux et territoriaux se sont penchés sur ces questions. Dans son récent rapport, intitulé *Enhanced Service Delivery Through a Common Client Identifier: Options and Opportunities*, le groupe suggère que le recours à un code d'identification commun (et sa base de données) comporte d'importants avantages. Il permettrait d'identifier les requérants légitimes avant le paiement des prestations, plutôt que d'appartier les données après la découverte d'une fraude et de devoir recouvrer les paiements irréguliers.

Les fiches E311 utilisées dans le couplage ne comprenaient pas d'avis public de communication des renseignements et d'utilisation pour la détection de fraudes éventuelles liées à l'assurance-emploi. Ni RHC ni Revenu Canada n'ont rendu compte publiquement de l'utilisation et de la communication des renseignements personnels, comme l'exige la politique du gouvernement sur le couplage des données. Revenu Canada a commencé à supprimer les détails non pertinents sur les fiches qu'elle communiquait à RHC lorsque le prestataire conteste le recouvrement des prestations d'assurance-emploi.

Le Commissaire a conclu que l'envergure du couplage et sa mise en oeuvre étaient excessives. Après qu'un important échange de lettres et la tenue de réunions avec les deux ministères, y compris au niveau ministériel, n'aient pas permis de résoudre le différend, le Commissaire a sollicité un avis juridique. Le Commissaire demande des conseils de la Cour fédérale sur la question de savoir si le fait de mener une recherche pour repérer tous les voyageurs de retour au pays lorsqu'on soupçonne une fraude de l'assurance-emploi enfreint les dispositions sur les fouilles, perquisitions ou saisies abusives (article 8) de la Charte.

qu'avait le Commissariat quant à l'utilisation de données rétroactives, le manque d'avis donné aux voyageurs au sujet de l'utilisation indépendante des données de douanes durant le projet pilote, et le manque d'accord écrit sur les modalités de l'échange. Le personnel du Commissariat a cru comprendre que toutes ces préoccupations trouveraient réponse avant la mise en oeuvre du projet. RHC a complété sa proposition de couplage des données à la fin de février, et le Commissariat a avisé le ministère, le 19 mars 1996, qu'il ne s'opposerait pas à l'exécution du projet pilote.

RHC a de nouveau obtenu de Revenu Canada les données qui avaient servi lors de l'étude de faisabilité et s'est contenté de les traiter de nouveau pour confirmer les chiffres obtenus. Au début de juillet 1996, il a fourni des copies de chaque dossier de demande de prestations d'assurance-emploi et des fiches E311 au représentant régional des prestataires concernés. Le bureau régional a achevé l'information au CEC pertinent, qui a écrit à chaque prestataire pour savoir pourquoi le prestataire avait réclamé des prestations d'assurance-emploi alors qu'il se trouvait en voyage. Revenu Canada n'a pas retiré des fiches E311 qu'il a fournies à RHC les renseignements qui n'étaient pas pertinents au projet.

Le projet pilote RHC considérait le retraitement des données ayant servi à l'étude de faisabilité comme la première phase de son projet pilote. C'est seulement en avril 1997 que les ministères ont signé un protocole pour le projet pilote. À la fin du projet pilote, RHC doit décider si le projet de couplage deviendra une opération permanente. Il continue à payer à Revenu Canada les coûts de l'équipement et des 30 employés pour la création de la base de données électronique. Revenu Canada communique maintenant aussi le but du voyage.

Depuis, Revenu Canada a fourni tous les mois à RHC des bandes informatiques contenant les déclarations des voyageurs canadiens durant les mois de décembre 1992, janvier à juin 1993, décembre 1994 et janvier à mars 1995. Bien que la période de conservation des microfiches E311 soit de deux ans, Revenu Canada les a conservées depuis 1992 pour aucune raison apparente sur le plan des douanes. Revenu Canada estime qu'environ 18 millions de voyageurs et de résidents rentrent au Canada par voie aérienne chaque année.

Les occurrences et les fichiers de demande sont envoyés au Centre des enquêtes de Miramichi aux fins de vérification et de suivi. RHC a pris des mesures relativement aux occurrences obtenues pour les demandes de date ultérieure à décembre 1994. Les prestataires ont été contactés et ceux qui n'ont pu justifier leur absence ont dû rembourser les prestations reçues pendant leur période d'absence, en sus d'une amende.

Les deux ministères ont consulté le Commissariat de façon officielle en juin 1995 pour discuter du projet de couplage. Compte tenu du fait que les preuves d'abus sont dans une large mesure, du genre anecdotique, le personnel du Commissariat leur a demandé de fournir des faits qui justifiaient le projet de couplage, y compris une analyse de coûts et avantages.

Le projet de couplage comprend quatre phases : une étude de faisabilité pour recueillir des données pour l'analyse des coûts et avantages, un nouvel examen de l'étude de faisabilité, un projet pilote de six mois et, en dernier lieu, une mise en oeuvre complète à la fin de 1997.

L'étude de faisabilité Pour recueillir les données nécessaires à une proposition officielle de couplage, Revenu Canada et RHC ont signé un accord en juin 1995 aux termes duquel Revenu Canada communiquerait à RHC les renseignements sur les voyageurs afin que l'étude de faisabilité sur la détection des fraudeurs de l'assurance-emploi puisse se dérouler.

L'accord prévoyait la communication à partir du 4 juillet 1995 des fiches remplies par les voyageurs. Revenu Canada recueillerait un échantillonnage de fiches provenant de neuf aéroports pour les mois de juin, septembre et novembre 1994 et les mois de février et mars 1995. RHC a accepté de ne pas prendre de mesures d'application de la loi à l'égard des personnes relevées lors du processus de couplage des données.

Puisque Revenu Canada conserve les déclarations des voyageurs sur microfiches, RHC a consenti à payer du personnel, travaillant dans les locaux de Revenu Canada, pour convertir l'information contenue sur les 16 861 échantillons en format électronique et la charger sur des disquettes. Les données comprenaient les nom, date de naissance, code postal, périodes de voyage des voyageurs, ainsi que les numéros de bobine et de feuillets des microfiches sur lesquelles les fiches E311 sont conservées.

Le couplage électronique a permis de relever 257 personnes qui étaient à l'extérieur du pays au moment où elles recevaient des prestations d'assurance-emploi, soit 1,5 p.100 de l'ensemble des échantillons. RHC a retourné les disquettes à Revenu Canada et a obtenu une photocopie des fiches E311 de ces 257 personnes.

Projet de couplage des données RHC a analysé les résultats de l'étude de faisabilité et a présenté un projet officiel de couplage des données au Commissariat en janvier 1996. Au cours de la réunion tenue pour discuter du projet pilote, le personnel du Commissariat a insisté sur les préoccupations

indirecte, et habituellement invisible, de données, le gouvernement a établi un processus de contrôle.

L'une des mesures est de fournir au Commissaire à la vie privée une étude de faisabilité préliminaire 60 jours avant le couplage. Cela permet au Commissaire, à titre de haut fonctionnaire du Parlement, d'agir comme défenseur des personnes dont on veut appier les dossiers. Le Commissariat examine le projet de couplage et fait ses recommandations à l'administrateur général du ministère, qui est libre de les accepter ou de ne pas en tenir compte. Le Commissaire n'a pas le pouvoir d'arrêter ou de modifier le projet.

Ce manque de pouvoir n'a pas posé beaucoup de problèmes jusqu'à maintenant; les ministères ont été sensibles à la question et ont en général accepté les recommandations du Commissaire. Mais les temps changent. L'introduction de la gestion fondée sur les résultats a amené les ministères qui fournissent des prestations importantes à adopter une approche dure. La plupart des contribuables les applaudiront. Le Commissariat, cependant, n'y voit pas que du bien, lorsqu'un appariement de données se fait sur une base si vaste qu'en plus de risquer d'enfreindre la *Loi sur la protection des renseignements personnels*, il menace des droits fondamentaux. Nous soutenons que le couplage des déclarations de douane des voyageurs et des fichiers des prestataires de l'assurance-emploi constitue un tel cas.

Il s'agit du couplage que le ministère des Ressources humaines Canada (RHC) a entrepris. RHC prend les renseignements inscrits sur le formulaire E311, Carte de déclaration des voyageurs, de Revenu Canada, et les apparie aux dossiers des prestataires de l'assurance-emploi pour déterminer si ces derniers ont retiré des prestations lorsqu'ils se trouvaient à l'extérieur du pays.

Déclaration de douane Tout voyageur qui rentre au Canada en empruntant un transporteur public (avion, train et autobus) doit remplir la fiche et la présenter à l'agent des douanes et de l'immigration au point d'entrée. Il y inscrit son nom, adresse et date de naissance, son numéro de vol et le nom de la compagnie de transport, qu'il arrive des États-Unis ou d'ailleurs, le nom des trois pays qu'il a visité lors de son séjour à l'extérieur; il précise aussi si le voyage a été entrepris par affaires ou pour des motifs personnels, le genre de produits qu'il ramène au Canada, s'il se rendra à une ferme dans les 14 prochains jours, la date de son départ du Canada, la date de son retour au Canada, la valeur des produits qu'il a achetés et l'exemption personnelle qu'il réclame. Un tampon des douanes identifie l'aéroport.

Rien à cacher et rien à prouver

On est loin d'exagérer lorsqu'on caractérise de voie vers l'établissement d'une société de surveillance les options qu'étudient actuellement les gouvernements. Il est naturel que les Canadiens considèrent, en général, que leurs gouvernements sont bienveillants; cela découle de notre sort privilégié. Notre géographie et notre climat exigent que nos gouvernements aient une conscience sociale, qui se reflète dans notre filet de sécurité sociale. Toutefois, l'existence de ce filet ne doit pas nous mener à abdiquer nos responsabilités civiques, dont l'une est de veiller à ce que la liberté personnelle et de choix de l'individu ne soit pas immolée sur l'autel de l'efficacité gouvernementale.

Les gouvernements ont maintenant les moyens de dépister à peu près tous les contacts qu'ont leurs résidents avec l'État; les données ainsi acquises sont versées dans de vastes bases de données et échangées sur une vaste échelle. Mais avec les moyens sont venues les pressions visant la réduction, la rationalisation et l'offre de services d'une manière plus efficace. Une partie de cette activité de collecte de renseignements constitue une activité légitime d'un programme gouvernemental, car il s'agit d'une utilisation conforme des données. Toutefois, d'autres aspects nous semblent perturbants, en particulier, l'appariement des déclarations de douanes des voyageurs revenant au Canada avec la base de données de l'assurance-emploi, dont l'une envergure est si considérable que nous la jugeons constituer un acte de perquisition et saisie déraisonnable aux termes de la Charte.

Nous examinons dans le présent rapport quelques-uns des développements de la dernière année : l'appariement des données de Douanes Canada et d'Emploi, les projets de cartes uniques, les numéros uniques et les bases de données exhaustives des programmes sociaux qui deviendraient communs à divers gouvernements, une base de données électronique nationale sur la santé, plusieurs registres de la population, la liste électorale permanente, le registre des armes à feu, la base de données des empreintes génétiques.

Mais il y a aussi une lueur d'espoir à l'horizon grâce au rapport exhaustif et vigoureux du Comité parlementaire sur les droits de la personne et traitant de l'impact des nouvelles technologies sur la vie privée.

Couplage des données Douanes et Assurance-emploi

Le couplage des données lie des données provenant de diverses sources indépendantes, presque toujours sous forme électronique, pour que des décisions administratives puissent être prises concernant les personnes qui utilisent des programmes et services gouvernementaux. Parce que ce couplage est une collecte

Baron Philippe

Quels que soient les gestes que nous posons pour protéger la vie privée, nous devons reconnaître l'importance de cette valeur, et penser aux conséquences que pourrait avoir le fait de considérer la vie privée, par négligence ou par aveuglement, comme une simple nuisance administrative qui entrave l'efficacité et les résultats financiers. C'est la voie qui mène à la société de surveillance. Je demande au gouvernement de ne pas s'y engager.

La protection de notre vie privée ne consiste pas à simplement débattre la valeur de l'intérêt personnel par rapport à un intérêt opposé. Le respect de la vie privée sert un intérêt collectif, commun et public. La vie privée, en tant que valeur, consolide notre société en renforçant, grâce au respect mutuel, notre sentiment de lien.

Il est peut-être temps d'envisager, comme le propose Priscilla Regan dans son livre *Legislating Privacy*, que le fait de considérer la vie privée comme un droit d'ordre individuel ne constitue pas une base solide sur laquelle asseoir l'ordre public. Nous devrions plutôt considérer l'importance sociale de la vie privée; sa place inhérente dans notre société démocratique; et comprendre comme le droit à la vie privée influe sur nos interactions personnelles et sur nos relations avec les organismes sociaux, politiques et économiques, ainsi que sur les pouvoirs que nous sommes disposés à leur consentir.

Dans une lettre qu'il nous adressait récemment, M. Whyte, de Toronto, soutenait qu'une telle pratique ouvre la porte à tous les abus de puissance informatique au gouvernement, et il incitait les citoyens à s'y opposer. Selon lui, bien que le couplage des données puisse paraître raisonnable et dans l'intérêt public, il pourrait servir de précédent au gouvernement pour utiliser les renseignements indiqués sur les déclarations de douane afin d'identifier les citoyens qui se sont rendus dans des pays dont le gouvernement réproouve les politiques, veut limiter le commerce extérieur, etc. Les régimes politiques autocratiques utilisent de façon courante l'information sur les déplacements pour exercer un contrôle sur leur population. Il ne faut pas admettre un tel précédent au Canada. Les Canadiennes et Canadiens doivent s'opposer, au nom de leur liberté, au couplage des données. M. White incite fortement les citoyens à mettre fin à cet usage répréhensible de données de douane.

Le « Panopticon » de l'information

En fait, un tel couplage est une version électronique du Panopticon de Jeremy Bentham, un philosophe du 18^e siècle. Ce dernier a proposé de concevoir une prison dans laquelle les gardiens observeraient les détenus à partir d'une tour centrale qui les cacherait au regard. La présence, ou l'absence, de gardiens dans la tour n'aurait pas d'importance, car une visibilité permanente et voulue serait ainsi créée et garantirait l'exercice automatique du pouvoir. Efficace... mais effrayant. Puisque la technologie permet désormais au gouvernement de créer son propre Panopticon informationnel, pourquoi ne s'en servirait-il pas? Si nous pensions que nos moindres gestes étaient observés, il se pourrait que notre comportement devienne sans reproche, ou à tout le moins différent. On ne doit pas sous-estimer le pouvoir de la peur et de la honte pour le contrôle d'une société et la suppression de l'autonomie individuelle. Mais il ne faut pas convenir, avec les bureaucrates, que notre société est corrompue à tel point que notre autonomie et notre vie privée doivent céder le pas à leur quête d'efficacité.

Vous allez me faire remarquer que, si vous n'avez rien à cacher, tout cela importe peu; et que, parfois, il arrive que les intérêts de la société doivent avoir préséance sur les droits de l'individu.

C'est peut-être sur ce point que nous nous égarons. Il est temps de penser aux ravages que l'exercice sans entraves du pouvoir peut infliger à notre société. En reléguant au statut de droit individuel le droit à la vie privée, nous sommes forcés de jouer coeur/à-tout, en termes de « ce droit prime sur cet autre » et « mon droit, en qualité de contribuable, a ne pas être roulé prime sur ton droit à ne pas être surveillé ».

maison, sans mandat, sans préavis, sans permission et sans soupçon précis. Les policiers pénétrèrent sans façon chez vous pour procéder à leur fouille. Combien de temps croyez-vous que les habitants de votre ville toléreraient un tel comportement?

Toutefois, dans notre monde informatisé, la technologie permet de faire précisément la même chose, soit de fouiller systématiquement chaque vie. Les gouvernements qui marient des données font entorse à la présomption d'innocence, puisque chaque personne est soupçonnée jusqu'à ce que l'ordonnateur l'innocente. Un ancien commissaire à la vie privée déclarait que c'était l'équivalent technologique d'une perquisition et saisie. Si nous permettons au gouvernement d'agir ainsi, il fouillera systématiquement les dossiers de tous ses citoyens afin de découvrir une trace de culpabilité.

Aucun commissaire à la vie privée ne peut accepter une fouille informatique qui fait fi de la présomption d'innocence, qui ne repose sur aucun soupçon raisonnable et qui n'est soumise à aucun mécanisme indépendant d'autorisation. Si de tels couplages deviennent chose courante, le gouvernement ne respecterait plus aucun des renseignements personnels des citoyens, que ces renseignements aient été fournis de plein gré ou sous la contrainte.

Comme nous n'avons pas réussi à convaincre les bureaucrates, ou leurs ministres, de modifier le couplage, nous avons sollicité l'avis de l'un des plus éminents juristes du droit constitutionnel au Canada. Ce dernier a renforcé notre position en soutenant qu'un tel couplage enfreint les dispositions de la *Charte canadienne des droits et libertés* traitant de perquisition et saisie. Le gouvernement et nous sommes en train d'étudier la façon la plus rapide dont nous pourrions saisir les tribunaux de cette cause.

Depuis le début de mon mandat, il y a six ans, c'est la question la plus cruciale dont j'ai été saisie. Je n'ai aucun intérêt, en tant que contribuable, à défendre les fraudeurs de l'assurance-emploi, mais j'ai tout intérêt à éviter que le gouvernement ne surveille, grâce aux moyens informatiques, des millions de contribuables respectueux des lois. La Charte défend tous les citoyens, individuellement et à titre de membres de notre société, d'avoir à prouver leur innocence. Les droits enchaînés dans la Charte ne devraient pas être mis en péril simplement parce que la technologie le permet.

Un tel couplage pourrait avoir des incidences énormes. S'il est permis, rien n'empêcherait de passer rapidement à un système de surveillance général où des renseignements personnels, à tous les paliers de gouvernement, sont échangés et couplés.

privée et annihilier la relation de confiance qui doit s'établir entre le citoyen, qui fournit l'information, et son gouvernement, qui l'utilise.

Compte tenu des pressions intenses qui s'exercent sur les ministères fédéraux pour qu'ils coupent dans le gras, et de la facilité qu'offrent les moyens informatiques pour le pistage des citoyens, une confrontation était probablement inévitable.

La question concerne une pratique adoptée par RHC, qui consiste à extraire des déclarations de douane de tous les voyageurs rentrant au pays par avion des données pour repérer les prestataires d'assurance-emploi qui se trouvaient à l'étranger. On s'attend à ce qu'une personne touchant des prestations soit à la recherche d'un emploi et soit disponible pour accepter un emploi; on s'attend aussi à ce que, si elle doit s'absenter de façon prolongée de son domicile fixe, elle le signale au ministère. Les agents de RHC (et nombre de contribuables) sont depuis longtemps irrités par des histoires, qui sont presque devenues des légendes urbaines, voulant que nombre de prestataires se paient des vacances aux frais du contribuable. Le ministère soutient qu'il est impuissant à mieux gérer le programme et à faire respecter la loi.

RHC a eu l'idée de comparer la liste des prestataires à celle des voyageurs, établie d'après les déclarations de douane, pour déterminer rapidement si certains des millions de voyageurs recevaient des prestations d'assurance-emploi, et s'ils avaient signalé leur absence.

Nul doute qu'une telle approche permettrait d'identifier certains prestataires malhonnêtes, mais ce serait chèrement payé, puisque des millions de voyageurs innocents seraient soumis à une surveillance systématique, à leur insu et sans leur consentement, après avoir rempli de bonne foi une déclaration de douane censée, s'ils en croient Revenu Canada, ne servir qu'à des fins de douanes.

Cette comparaison par le couplage enfreint le principe le plus fondamental de toute loi sur la vie privée, à savoir que le gouvernement doit révéler aux citoyens pourquoi il recueille des renseignements personnels, puis n'utiliser ces renseignements qu'à la seule fin pour laquelle il les a recueillis, et non à une fin totalement distincte (sauf avec le consentement écrit du citoyen). Ce principe est clair : il s'agit d'éviter que le gouvernement ne surveille ses citoyens de façon abusive en fouillant, parce que la technologie le lui permet, dans ses énormes bases de renseignements personnels.

Prenons un exemple où n'intervient aucun ordinateur. Supposons que certains criminels séjournent dans votre ville, et que la police décide de fouiller chaque

sur la protection des renseignements personnels. Nous nous réjouissons de cette promesse, et nous attendons avec impatience qu'elle se concrétise.

En dernier lieu, nous sommes heureux de constater qu'un nombre croissant de ministères fédéraux sollicitent nos conseils et nos commentaires sur leurs projets qui ont une composante de vie privée. Nous attirons l'attention, dans notre dernier rapport, sur la collaboration fructueuse qui s'était établie avec le Directeur général des élections pour assurer le respect des droits des Canadiennes et Canadiens en matière de protection de leurs renseignements personnels lors de l'élaboration de la liste électorale permanente.

D'autres gros utilisateurs de renseignements personnels, notamment Statistique Canada et Ressources humaines Canada (RHC), ont sollicité notre apport lors de projets de grande envergure. RHC, en particulier, a plusieurs projets à l'étude, dont un porte sur la mise au point d'un code d'identification commun du client, ressemblant à un numéro d'identité universel, et a donc de nombreuses incidences sur la vie privée. D'autres projets mettront à l'épreuve la théorie selon laquelle la technologie et le respect de la vie privée peuvent coexister. Nous les suivrons de près.

Les ministères fédéraux ne sont pas tenus de consulter le Commissariat. Mais notre personnel, armé de compétences et connaissances, peut aider de façon très utile les ministères fédéraux à réaliser leur objectifs de politique et de gestion d'une façon qui respecte les droits des Canadiennes et Canadiens. Le Comité présidé par Mme Finestone a reconnu la valeur de cette fonction de consultation et a recommandé qu'elle soit enchâssée dans le mandat du Commissariat.

D'autre part ...

Si je pouvais m'arrêter ici, l'année qui vient de s'écouler n'aurait effectivement été jalonnée que de progrès. Mais toute médaille a un revers.

Nous abordons maintenant une pratique qui constitue une menace absolue à la vie privée et à son corollaire, l'autonomie. Cette pratique nous a menés à confronter deux gros ministères fédéraux, soit Ressources humaines Canada et Revenu Canada, et elle a précipité un recours aux tribunaux, lesquels pourraient, en définitive, être appelés à établir si la vie privée est une valeur fondamentale de notre société, ou un simple irritant à ranger au nombre des bonnes intentions inaccomplies en raison de son caractère trop épineux.

La question controversée porte sur le couplage de données, une activité qui, de prime abord, paraît inoffensive, mais qui pourrait signer l'arrêt de mort de la vie

L'étendue et la profondeur du rapport, intitulé *La vie privée : où se situe la*

frontière, qui a été diffusé en avril peu avant la dissolution de la Chambre en

prévision de l'élection fédérale, coupent le souffle. Il se distingue des rapports

antérieurs par le fait que la vie privée y est reconnue comme valeur fondamentale de la société canadienne, et non comme monnaie échangeable contre des

avantages sociaux ou économiques. Un membre du Comité considérerait que la vie privée est un droit associatif, c'est à dire un droit essentiel à la liberté

d'expression et d'association, et qui est au cœur même de notre autonomie. Le

rapport offre des lignes directrices pour cerner l'impact, du point de vue social et éthique, des nouvelles technologies.

Le ministre de la Justice frapperait un grand coup s'il fondait les grandes lignes de la loi qu'il a promise sur le travail du Comité, sur celui du Conseil consultatif sur l'autoroute de l'information (visant la protection de la vie privée dans les réseaux en ligne) et sur le code modèle sur la vie privée de l'Association canadienne de normalisation.

Le rapport du Comité mérite plus que le tiède accueil qu'on lui a fait.

Un autre développement important, cette fois sur la Colline du Parlement, a été l'adoption unanime par les députés de la motion émanant de Paul Crête, député de Kamouraska-Rivière-du-Loup, qui vise à étendre les dispositions de la *Loi sur la protection des renseignements personnels* à toutes les sociétés de la Couronne. C'est une mesure qui a été préconisée par le Commissariat à plusieurs reprises, ainsi que par le Comité de la Chambre des communes sur la justice lors de sa révision de la *Loi sur la protection des renseignements personnels* en 1987. Cette motion, même si elle n'a pas force de loi, est une expression manifeste, par toutes les parties, de l'orientation que doit prendre le gouvernement et une indication claire que les députés sont de plus en plus conscients des préoccupations de la population en matière d'atteintes à la vie privée.

Le gouvernement s'est aussi enfin rendu à nos arguments répétés de mettre fin à l'effritement du droit à la vie privée causé par ses efforts pour élarguer dans ses dépenses. La transformation de ses opérations en organismes à but non lucratif, monopoles commerciaux et compagnies compétitives privatise les employés et les clients des droits à la vie privée dont ils jouissaient aux termes de la *Loi sur la protection des renseignements personnels*.

Après une période d'hésitation, durant laquelle les services de contrôle de la navigation aérienne ont été confiés à l'entreprise privée (NAV CANADA), sans que les droits précités ne le soient, on nous a promis une nouvelle politique qui étendrait à tous les organismes nouvellement privatisés les dispositions de la *Loi*

D'une part ...

Paradoxe n.m.—antinomie, contradiction entre deux idées, deux principes, deux propositions. (*Petit Larousse*)

Dans le cas présent, c'est la protection de la vie privée qui constitue un paradoxe au sein du gouvernement du Canada, dont les messages à ce sujet ont été contradictoires et ont prêté à confusion. Au cours des dix dernières années, certains des développements les plus prometteurs et stimulants ont coïncidé avec certains des développements les plus perturbants et dangereux.

Nous avons noté que le besoin urgent de lois plus fortes et complètes pour protéger le droit à la vie privée des Canadiennes et Canadiens est de plus en plus reconnu, mais que certaines initiatives le menacent. Qu'est-ce qui l'empêtera?

Accolades

La promesse faite par le ministre de la Justice, Allan Rock, à l'effet que d'ici à l'an 2000, une loi protégeant, de façon réelle et exécutoire, la vie privée au sein du secteur privé serait en place a été un événement d'une importance fondamentale. Le gouvernement a reconnu que la technologie rend impossible le maintien d'une protection efficace de la vie privée si la loi ne s'applique pas autant au secteur privé qu'au secteur public.

Le Commissariat préconise depuis fort longtemps une telle mesure, qui est aussi appuyée par le Conseil consultatif fédéral sur l'autoroute de l'information, l'Association canadienne du marketing direct, et les Commissaires à l'information et à la vie privée du Québec, de l'Ontario et de la Colombie-Britannique, pour n'en mentionner que quelques-uns. Nous ne pouvons qu'espérer qu'il restera suffisamment de vestiges de vie privée à protéger au tournant du siècle.

Il est singulier de constater que l'annonce du ministre Rock, qui constitue la plus importante déclaration fédérale sur la vie privée depuis l'adoption, en 1983, de la *Loi sur la protection des renseignements personnels*, a suscité peu de réactions au sein des médias canadiens, lesquels portent en général un intérêt soutenu au domaine de la vie privée.

Cette observation s'applique aussi à une étude très importante, faite par le Comité de la Chambre des communes sur les droits de la personne, présidé par l'honorable Sheila Finestone. Le Comité s'est penché pendant près d'un an sur l'impact des nouvelles technologies sur la vie privée; il a tenu des séances dans plusieurs villes du pays et il a consulté un grand nombre de témoins représentant une gamme complète d'opinions.

Table des matières

D'une part ...	1
D'autre part ...	3
Rien à cacher et rien à prouver	8
Service tout en un : le code d'identification commun	13
Un dossier médical électronique... et national!	17
Registres de la population	23
La liste électorale permanente	23
Le registre des armes à feu	26
Banque de données génétiques	29
Jusqu'où le Parlement doit-il aller?	34
Privatisations et cessions de responsabilités : Que reste-t-il ?	37
Diffusion de l'identité des criminels dangereux—mise à jour	41
Actualité en télécommunications	44
Devant les tribunaux	47
Incidents	49
Vérifications	56
Notification du Commissaire	60
Direction des enquêtes	64
Cas	66
Demandes de renseignements	79
Conférence internationale des commissaires à la vie privée à Ottawa	87
La protection des renseignements personnels au Canada—mise à jour	89
Direction de la gestion intégrée	92
Organigramme	94

Septembre

- Lors de la 18^e conférence internationale des commissaires à la vie privée, le ministre de la Justice du Canada s'engage à faire adopter une loi sur la protection des renseignements personnels dans le secteur privé (page 91)
- Comparution devant le Comité de la Chambre des communes sur les finances au sujet du livre blanc sur les institutions financières
- La Commission d'enquête sur les droits de la personne de l'Ontario décide que le programme de dépistage de substances d'une grande compagnie est illégale

Octobre

- Comparution devant le Comité permanent sur la procédure et affaires de la Chambre au sujet de la liste électorale permanente (page 23)
- Premières plaintes concernant l'appariement de données des ministères des Douanes et des Ressources humaines
- Documents fiscaux trouvés dans un classeur dans un magasin d'articles excédentaires du gouvernement (page 52)

Novembre

- Comparution devant le Comité permanent des modifications législatives de l'Assemblée législative du Nouveau-Brunswick au sujet d'un projet de loi sur la protection des renseignements personnels
- Postes Canada porté sur des cartes de crédit des produits non commandés (page 53)

Décembre

- Le CRTC annonce des audiences sur les frais de confidentialité du numéro de téléphone (page 46)

Janvier 1997

- Le ministère des Ressources humaines demande au Commissariat d'étudier les initiatives sur la main-d'oeuvre conclues avec des bandes indiennes

Février

- Comparution devant le Comité conjoint spécial sur un code de conduite pour les députés
- Le Forum national sur la santé appuie une base de données nationale sur les renseignements de santé (page 17)
- Comparution devant le Sous-comité sur les règlements aux termes de la Loi *sur les armes à feu* (page 26)

Mars

- Le Comité sur les droits de la personne tient des audiences à travers le pays sur la protection des renseignements personnels et la technologie
- Transports Canada et les fichiers du système de navigation aérienne (page 59)

Survol de l'année

Avril 1996

- Comparution devant le Comité de la Chambre des communes sur les services de transport au sujet du projet de loi C-20, concernant la privatisation du système de navigation aérienne (page 38)
- Postes Canada photocopie les adresses d'acheminement de ses concurrents (page 50)
- Le Commissaire répond au document du Solliciteur général concernant la base de données des empreintes génétiques (page 29)

Mai

- Réunion des commissaires canadiens à la vie privée à Victoria, en C.-B.
- Dossiers de Santé Canada trouvés dans un bac à ordures à Winnipeg (page 51)
- Le Conseil consultatif sur la route de l'information en faveur d'une loi cadre sur la vie privée d'ici à l'an 2000
- L'Association canadienne du marketing direct appuie le plan du gouvernement d'étendre au secteur privé les dispositions de la Loi sur la protection des renseignements personnels

Juin

- Recensement
- Le Comité de la Chambre des communes sur les droits de la personne et la condition des personnes handicapées tient une table ronde sur la protection des renseignements personnels et les nouvelles technologies (page 34)
- Le Cabinet ordonne aux compagnies de téléphone locales de communiquer les bases de données sur leurs clients aux éditeurs indépendants d'annuaires (page 44)
- Comparution devant le Comité de la Chambre des communes sur la justice et les questions juridiques au sujet des activités.
- Apparemment pilote de toutes les déclarations de douanes des voyageurs de retour au Canada et de la base de données sur l'assurance-emploi (page 8)
- Le CRTC délivre une licence au premier système de communications personnelles (page 45)

Juillet

- Le Groupe consultatif sur la protection des renseignements personnels considère un projet de loi sur la protection des données
- La Cour fédérale refuse l'accès aux notes des membres du Conseil canadien des relations de travail (page 47)

Août



Commissaire
à la protection de
la vie privée du Canada

Privacy
Commissioner
of Canada

L'honorable Gilbert Parent
Président
Chambre des communes
Ottawa

juillet 1997

Monsieur,

J'ai l'honneur de soumettre mon rapport annuel au Parlement. Le rapport couvre la période allant du 1^{er} avril 1996 au 31 mars 1997.

Veillez agréer, Monsieur, l'expression de mes sentiments respectueux.

Le Commissaire,

Bruce Phillips



Commissaire
à la protection de
la vie privée du Canada

Privacy
Commissioner
of Canada

L'honorable Gildas L. Molgat
Président
Sénat
Ottawa

juillet 1997

Monsieur,

J'ai l'honneur de soumettre mon rapport annuel au Parlement. Le rapport couvre la période allant du 1^{er} avril 1996 au 31 mars 1997.

Veuillez agréer, Monsieur, l'expression de mes sentiments respectueux.

Le commissaire,

Bruce Phillips

Le Commissaire à la protection de la vie privée du Canada
112, rue Kent
Ottawa (Ontario)
K1A 1H3

(613) 995-2410, 1-800-267-0441
Téléc. (613) 947-6850
ATS (613) 992-9190

© Groupe communication Canada
N° de cat. 30-1/1997
ISBN 0-662-63040-8

Cette publication est offerte sur cassette et sur disquette informatique. Nous sommes accessibles sur le réseau Internet à : <http://infoweb.magi.com/~privcan/>

Rapport annuel du
Commissaire à la protection
de la vie privée
1996-1997





RAPPORT ANNUEL 1996-1997

COMMISSAIRE À LA PROTECTION DE LA VIE PRIVÉE





Privacy Commissioner

1997-98 annual report

CAI
PC
- A57



Privacy Commissioner

1997-98 annual report



The Privacy Commissioner of Canada
112 Kent Street
Ottawa, Ontario
K1A 1H3

(613) 995-2410, 1-800-267-0441
Fax (613) 947-6850
TDD (613) 992-9190

© Minister of Public Works and Government Services Canada 1998
Cat. No. IP 30-1/1998
ISBN 0-662-63685-6

This publication is available on audio cassette, computer diskette and on the Office's Internet home page at <http://infoweb.magi.com/~privcan/>



Privacy
Commissioner
of Canada

Commissaire
à la protection de
la vie privée du Canada

July 1998

The Honourable Gildas L. Molgat
The Speaker
The Senate
Ottawa

Dear Mr. Molgat:

I have the honour to submit to Parliament my annual report which covers the period from April 1, 1997 to March 31, 1998.

Yours sincerely,

A handwritten signature in blue ink that reads "Bruce Phillips".

Bruce Phillips
Privacy Commissioner



Privacy
Commissioner
of Canada

Commissaire
à la protection de
la vie privée du Canada

July 1998

The Honourable Gilbert Parent
The Speaker
The House of Commons
Ottawa

Dear Mr. Parent:

I have the honour to submit to Parliament my annual report which covers the period from April 1, 1997 to March 31, 1998.

Yours sincerely,

A handwritten signature in blue ink that reads "Bruce Phillips".

Bruce Phillips
Privacy Commissioner

Table of Contents

Some Unfinished Business	1
A Private Sector Privacy Law	11
Protecting Health Information	18
Investigations and Inquiries Branch	21
Cases	22
Inquiries	45
Tables and Charts	46
A Better Window on Privacy:	
Managing policy and research	56
A Marketer's Dream — A Privacy Nightmare?	58
Can We Keep a Secret?	60
Stick Before Carrot —	
Policy on using electronic networks	63
Internet — Still No Privacy	65
But a Useful Tool	69
The DNA Databank Bill — Still	73
The Year on the Hill	75
Updates:	79
Private Directories: the end of the saga, Permanent Electors Register, A Sharing Agreement Becomes Visible	
Data Matching Notifications:	85
Canada Student Loans with Government Employee Database, Alberta Disability Income Program with CPP Disability Claimants, Old Age Pension and QPP Death Notices, OAS and QPP Claimants	
In the Courts:	
Cases, The Charter — a reasonable expectation of privacy	89
Privacy Protection in Canada — an update	99
Corporate Management	102
Organization Chart	104

Some Unfinished Business

This annual report marks both the end of my seven-year term and the beginning of a two year extension. It seems an appropriate moment to express my gratitude to Parliament for this opportunity to deal with two pressing issues. The first is seeing an effective and enforceable privacy law in place in the private sector. The second: ensuring that the planned health information infrastructure does not lead to open season on patients' medical information. About which, more in a moment.

Certainly the information landscape has been transformed during this term but it is a transformation well underway seven years ago. Computer technology led the revolution in information management, bringing with it all the promise and peril of massive new collection and use of personal information. All the prophecies made at the time, both for good and for ill, have been borne out. The personal information of millions of people is being collected, manipulated, massaged, bought and sold, used and abused at a rate now many times faster than was possible seven years ago.

We have seen the maturation of perhaps history's greatest and potentially most liberating communications system, the Internet. Millions more users join the Net each year, and surely it will soon become as much a commonplace as — and may well supplant — the telephone for much of the world's commercial transactions and personal communications.

But Internet has also brought new problems; threats to privacy, decency and truth (and possibly to individual safety). With the abuses comes a corresponding effort by society generally, and governments particularly, to gain some control. Some of these efforts, such as those aimed at eliminating the traffic in pornography, are entirely commendable. Others are unappealing. One of the latter is the government's appetite to control and override encryption, the most-promising technique for assuring adequate privacy for individual users and security for electronic commerce. Strong-arm initiatives such as these might well prove a suffocating inhibition, and destroy much of Internet's value as an open and wonderfully flexible method for the world to communicate.

Meantime, the drift toward increasing surveillance of our society has become a flood. Almost every day, we read of more spy-cameras in another community. More streets, more businesses, more workplaces are subjected to the baleful stare of these electronic Little Brothers. As usual, the surveillance is done in the name of greater security and safety. Sometimes it may even be justified. More often it is not, witness the recent decision of one bar owner to install cameras to record the unruly behaviour of some patrons.

This pervasive surveillance signals a rapid approach to rock-bottom in our respect for individual rights. Easier to resort to a quick surveillance fix and diminish everyone's right to some private enjoyment, rather than accept responsibility for maintaining a civilized atmosphere by refusing admission to, or turfing out the rowdy. But even more depressing is our uncritical acceptance of this spreading surveillance. We can achieve perfect safety and security to be sure. And, of course, we have nothing to hide. All we have to do is give up any notion of personal freedom.

On the Road to Damascus

The past seven years have brought one signal change; that is in my views on how best to face the mounting challenges to preserving privacy rights. My first annual report expressed a scepticism about the need for stronger privacy laws and "some hope yet for the path of voluntary action".

That hope did not long survive. By 1995 I confessed "Reluctantly, and by stages" to having concluded that "voluntarism is inadequate". I pressed for both federal and provincial action to bring the private sector under the umbrella of privacy laws. (Quebec had already done so).

This evolution in thinking occurred partly (but not entirely) because of the inadequate response of the private sector. Other important influences were at work. These include growing government and private sector exchanges of information, privatization of government operations with the resulting loss of existing privacy protection, and the developing European Union common data law which risks restricting information flow to countries with inadequate private standards — of which Canada is one.

By 1996, the government had reached the same broad conclusions. This happy event perhaps was not born solely out of concern for an individual right, but also due to a determination to see Canada ahead of the pack in developing electronic commerce. One is an inevitable consequence of the other; Canadians will not shop, bank and file taxes on line knowing they risk sharing their lives with more than 40 million people.

While we may quibble over the motivation, we welcome this means to our end. With the support of this office, other privacy commissioners and advocates and, above all, its own appointed Information Highway Advisory Council, the government committed itself to bringing in what then-Justice Minister Allan Rock described as “effective and enforceable” privacy laws in the private sector by the year 2000.

Industry Canada and the Department of Justice issued a discussion paper, *The Protection of Personal Information — Building Canada’s Information Economy and Society*, and called for public input. The departments are now digesting the responses (including ours — see page 11) and distilling their findings into a draft bill, aiming at publication in October, 1998

It is no exaggeration to call this the most important and promising Canadian development in privacy protection since the government’s 1971 report *Privacy and Computers* (which set the stage for the first privacy protection law in Part IV of the *Canadian Human Rights Act*). A good bill, living up to Mr. Rock’s “effective and enforceable” objective, will place Canada among the world’s leaders in defence of basic privacy rights. A bad one, studded with exceptions, exemptions and loopholes — and absent effective independent oversight — would be a disaster.

This office thus lives in high if somewhat nervous hopes. We observe powerful lobbies being organized by some elements of the private sector. And we have healthy if grudging respect for their ability to obtain favourable treatment for their special interests.

Another hurdle for this gestating legislation is the belief in some quarters that nothing effective can be done unless federal and provincial governments act together. It is true that much business falls under provincial jurisdiction. And it is evident that a harmonized approach and laws are extremely desirable. Consistent national standards would

make life easier for both business and government, understandable for individuals and avoid the spectre of data havens within the federation. This is the ideal. Nevertheless, if others cannot be convinced to protect their citizens' privacy rights in the marketplace, then the federal government must lead by example; a role the federal government seems poised to fill. The spotlight now shifts to the provinces which have jurisdiction over much of the private sector.

A Medical Internet?

Our other major preoccupation is the fate awaiting the management of Canadians' medical files. It is difficult to imagine any issue that conveys as much potential danger to privacy and confidentiality as the current efforts to create a national health information system. The system promises to make available the health information of virtually the entire population on-line for armies of health professionals, bureaucrats and researchers. A leak from a doctor's office is damaging enough; maintaining a trusted relationship with the health system's cast of thousands in quite another.

Work on this project continues apace, animated by a special federally-appointed advisory council whose membership includes no privacy specialists. Surprisingly little public attention has attached to this project considering how it will touch the lives of all of us.

The forces driving this project are several. They include the health bureaucracy at all levels — federal, provincial/territorial and municipal — which anticipates substantial cost savings, better anti-fraud controls, more efficient delivery of services. But they are not alone: health researchers argue that a more complete profile of the state of Canadians' health will lead to greater progress in all fields of medicine, particularly preventive.

Canadian doctors, however, while conceding some potential benefits, are extremely concerned. They fear the possible erosion, if not destruction, of the basic ethic of their profession: absolute confidentiality of the patient-doctor relationship. On that account, the Canadian Medical Association has devised a comprehensive privacy code which posits as its basic principle the need to obtain patient consent for almost every form of informational exchange. The draft is thoughtful and thorough.

Should it stand it will be nothing less than a Hippocratic Oath for the information age

This is a critical step at a crucial point in the evolution of health information management. It obliges proponents of a national health system to bring forward a proposal which meets decent privacy standards or risk the united opposition of the medical community.

It must be said that the advisory council is well aware of the privacy issue. The Co-chairman, Dr. Tom Noseworthy of Calgary, has publicly committed himself to a high level of privacy protection and, naturally, he enjoys the whole-hearted support of this and similar offices in its pursuit. But it would be naive and unrealistic to underrate the difficulties and complexities implicit in creating such an intricate web of health information exchanges in a way that protects the right of individuals. It bears repeating: the corollary of a publicly funded health care system is not abdication of that bedrock principle of our right to a confidential relationship with our doctors.

We therefore offer this advice: Use the privacy expertise already available to the maximum. Get it right the first time and public (and privacy commissioners') support will follow. Fail, and eroding public confidence will take the system down with it.

We follow the progress of this work with anxious care, firm in our conviction that if it cannot be done without the wholesale abolition of existing rights, it ought not to be done at all.

A sidebar to the CMA's promising code, and an early indication that health information codes are both desirable and do-able with members' commitment, is the new privacy component of the Canadian Dental Association's Code of Ethics. The Code (which is enforceable in some provinces) establishes dental patients right to seek dental care in "a confidential setting free of third-party intrusion". Patients have the right to examine and copy their records, control disclosure, and know with whom the information may be shared (with their consent). Third parties (such as Revenue Canada or insurance companies) may only access patient records for audits after identifiers and unrelated health information have been removed. This laudable effort underscores the CDA's ongoing commitment to its patients' interests. Members will not be sorry.

Updating the Privacy Act: another Year 2000 challenge

Perhaps lost in the shadow of these grand projects is the now-pressing need to modernize the existing *Privacy Act*. The act controls only the information handling of many — but not all — federal government agencies. It was a good bill in its time; major aspects of it have stood well the test of the last 15 years. However, the changing nature of privacy threats has also exposed some flaws and weaknesses.

The primary one of which is the law's focus on protecting information. It is not truly a privacy law but a data protection statute. In fact privacy has surprisingly little protection in Canadian law; torts in some provinces and — as a last resort — the Charter (see page 91). If it needs a road map to comprehensive privacy protection, the government need look no further than last year's report, *Privacy: Where Do We Draw the Line*, issued by the Commons Committee on Human Rights.

But to focus on the current act: first we need to clarify the definition of “personal information” to bring it up to speed with new technology. For example, DNA samples — tissue, blood, semen — should be defined as personal information for the purposes of the Act. And the Act needs more precision in its definition of what information about public servants “relates to the position or functions of the individual”. A clear definition might have avoided costly Court cases like those dealing with access to weekend sign-in sheets and parking privileges.

The Act's provisions establishing a person's right to access his or her personal records, and to require consent before disclosing personal information, are hedged round with numerous exemptions and exceptions which beg review. Most exemptions are justified. For example, it makes no sense to allow a person under investigation for a criminal offence to be allowed access to investigative records. Nor would one allow suspected terrorists to examine their records in CSIS files. But some exemptions are altogether too all-inclusive.

Section 22(1)(a) of the Act, for instance, authorizes federal investigative bodies to refuse to disclose information “pertaining to the enforcement of any law of Canada or a province”. This is sufficiently sweeping as to permit nine investigative bodies to refuse to release virtually all personal information.

I find particularly offensive the notion that departments can withhold information from applicants simply because the law allows it, even though disclosure would cause no demonstrable injury. All exemptions should be subject to an injury test, meaning investigative bodies should be required to demonstrate how granting access to an individual would harm a law or their investigations.

Next, given the fundamental importance of Sections 4 to 8 (the fair information code), Parliament should expand individuals' rights to appeal to the Courts about government collection, use and disclosure of personal data. This could include injunctive rights, or a privacy tort allowing individuals to sue for damages.

Also needed is a much tighter concept of the notion of "control" of personal records. This would prevent government institutions from circumventing the act by contracting out such products and services as investigations and surveys, or distancing themselves from personal records such as board members' notes.

Another serious weakness in the Act lies in information-sharing agreements and arrangements between the federal government and other levels of government (including governments of other nations), and the private sector. Many of these agreements are essential for the conduct of government operations, and are authorized by many statutes, including the *Privacy Act*. However, the scope of sharing permitted by the Act's broad language is an open barn door for even the slowest horse. There are hundreds of such agreements in existence, of which this office has only fragmentary knowledge. But what we do know is not comforting. Much of the sharing is virtually invisible to taxpayers, and often to the departments themselves.

Also, given the routine and detailed exchanges underway, it is essential that federal departments be required to ensure that any personal information they disclose enjoys proper privacy protection in the hands of the recipients. At a minimum, the Act should require departments to obtain a contractual commitment to provide privacy protection equivalent to that offered by the federal *Privacy Act*, coupled with a right to take those measures necessary to ensure that the commitments are honoured. Similar legal requirements should be placed on any private enterprise taking over any program or activity previously conducted by the government of Canada.

The government has responded in part. The Treasury Board has directed departments to include in privatization agreements some protection for the personal information being transferred. New bodies which remain in federal jurisdiction will be subject to the *Privacy Act*. Organizations that are privatized and come under provincial jurisdiction will have privacy clauses written into the sale contract.

Time for some housekeeping

There is also an urgent need to review the powers and mandate of the Office. In the beginning, the Office functioned principally as a complaint investigation bureau. That remains its primary statutory duty — and the only one for which it is funded. But the intervening years have imposed many new demands on the office not contemplated by the *Privacy Act*. One of these is the capacity for policy analysis and research so essential to keeping Parliament and the public abreast of important privacy developments: this was the term of Internet, digital fingerprinting, datamining and the National Health Information Infrastructure. This Office would be irrelevant to both legislators and taxpayers without such a service, one we struggle to provide now without any resources or legal mandate.

Even our core investigation function is under serious strain. During this seven year term, the size of the office remained virtually static, despite a complaint load now more than twice as large as at the outset.

Similarly, there is a growing public appetite for more information about the impact of technology on society. While Parliament may not have anticipated the public turning to us for answers, no-one told the public — witness the explosion of inquiries in the period. This Office has no mandate for public education, and thus no funding.

Nevertheless, we strive to meet these demands, conscious only that our best efforts are a marginal response at best.

These problems were examined and solutions proposed in a review of the Act by the Commons Justice Committee in 1987, then again in the special report *Privacy: Where do We Draw the Line*. No action so far, although the Justice Department, which is responsible for privacy law, has been considering amendments during the last two years. One can only wish that these particular judicial mills did not grind quite so slowly.

This review concludes with a footnote; a seven-year itch which the Commissioner would now like to scratch. Repeatedly during this period proposals have bubbled up to “merge” the Offices of the Information and Privacy Commissioners. Although the idea has been repeatedly stoked and fed by others, I have held my public peace, thinking it better to mind my own business and hoping that others would mind theirs.

It is time now to put this issue to bed. Privacy and access to information laws are not flip sides of the same coin. They have this in common: both provide Canadians right of access to records held by the federal government. But there the similarity ends. Access by definition is the limit of the *Access to Information Act* — does the applicant get the records or not? And, if the records at issue are personal, they are governed by the *Privacy Act*.

Otherwise, the two acts have about as much in common as soccer and succotash. Access to general government records is an administrative right, recently taking root in modern democracies, which sets out terms under which citizens can see government files. But many democracies do not have such laws. Privacy, however, is a core value, a basic human right which touches almost every aspect of life. It is, as the Supreme Court of Canada has said, a basic element in establishing individual freedom. Such is the freedom this office works to preserve. Indeed, all modern democracies protect the value in law and appoint an arbitrator/overseer. Only in Canada — and only in the provinces — does that arbitrator wear both the privacy and information hats.

The coming of private sector legislation and the Office’s possible role in its oversight makes the time ripe for a clean amicable divorce. Business needs to know that the regulator has but one priority and that is its handling of the personal information of its clients and employees. There can be no suspicion that a single commissioner might have an interest in general records.

Finally Parliament needs to fix an unforeseen weakness in the structure, reporting mechanism and accountability of the Office which have a debilitating effect.

The Privacy Commissioner’s office is an orphan. Despite his status as a Parliamentary officer, Parliament makes only occasional and cursory

examination of the issues and our operations. The budget is set as part of the Department of Justice envelope. Thus my only avenue of budgetary appeal is to ask the Minister of Justice (whose operations I may have to investigate) to beggar her own program. This arrangement sends all the wrong messages about the Office's independence and makes the principals profoundly uncomfortable. It is time the Act established a clear line of responsibility and accountability to Parliament, and it may also be the moment for Parliament to consider a consistent reporting and funding regime for all its officers.

Finally, allow me to give public expression of profound gratitude to an exceptional staff of devoted colleagues. Whatever credit accrues to this Office, or to me personally, is due to their high sense of purpose and professionalism. No commissioner was ever better served by or more deeply indebted to his staff.

A Private Sector Privacy Law

Comprehensive legislation to protect personal information in Canada's private sector has been both long needed and much anticipated. However, until very recently, private sector legislation appeared destined to be the perennial bridesmaid of the legislative process, always hovering near the altar, but never quite getting there. Now there is renewed hope, largely due to two initiatives.

The first is the government's discussion paper, entitled *The Protection of Personal Information: Building Canada's Information Economy and Society* which was released in January 1998. The paper sought public comment on a proposed model for legislation to protect personal information in the federally-regulated private sector. The second is a draft Private Sector Protection of Personal Information Act now being prepared by the Uniform Law Conference of Canada which could serve as the basis for consistent private sector law across Canada.

The history of attempts to bring private sector data protection legislation to Canadians dates from the early 1980s. When the bill that became the federal *Privacy Act* was introduced for third reading in June 1982, the then-Minister of Communications observed that "the next stage in the development of privacy legislation, [is] extension of the principles respecting the protection of personal information to the federally-regulated private sector." Since then, protection of personal information in the private sector has raised its head several times:

- In March 1987, the Standing Committee on Justice and Solicitor General endorsed private sector legislation in its report, *Open and Shut: Enhancing the Right to Know and the Right to Privacy*.
- In May 1996, the federal Industry Minister announced that consultations with the provinces and other "stakeholders" would be undertaken to bring forward proposals for a "legislative framework governing the protection of personal data in the private sector."
- In September 1996, then-Justice Minister and Attorney General Allan Rock announced that "by the year 2000, we aim to have federal legislation on the books that will provide effective, enforceable protection of privacy rights in the private sector."

- In April 1997, the House of Commons unanimously endorsed a private member's motion by Mr. Paul Crête to extend the existing *Privacy Act* to cover all Crown corporations.
- In April 1997, the Standing Committee on Human Rights and the Status of Persons with Disabilities produced a report entitled *Privacy: Where Do We Draw The Line?*; the report recommended that the current *Privacy Act* be replaced with a Data Protection Act that would extend privacy protection to personal information held by Parliament, all federal government departments, agencies, Crown corporations, boards, commissions and other institutions, as well as all federally-regulated businesses and industries.
- In March 1998, the Uniform Law Conference of Canada, an independent and non-governmental body, released its most recent draft of a uniform Private Sector Protection of Personal Information Act.

The government's proposal: a good start

Given the national nature of the private sector privacy issue, the responsibility naturally falls on the federal government to exercise leadership. Fortunately, major sectors of commerce such as banks, communications and transportation, fall squarely within the federal government's jurisdiction — three sectors which are among the most important collectors and users of personal information. Now, more than fifteen years after first publicly raising the prospect of protecting personal information in the federally-regulated private sector, the federal government is preparing to draft legislation.

The joint Industry Canada/Department of Justice discussion paper describes the present state of privacy law in Canada and why it is insufficient to protect Canadians in the current environment. It establishes the basic principles of effective privacy legislation, then discusses some options for implementing such a law and providing independent oversight. However, the paper's thrust is less about protecting personal information than it is an encouragement to feel confident in engaging in electronic commerce. It is revealing that the paper's introductory quotation, from the September 1997 Speech from the Throne, makes no reference to privacy or data protection.

Legislation to govern the federally-regulated private sector is important for several reasons. The distinction between the private and public sectors is blurring. Increasingly the federal government, like many others, is privatizing, commercializing and contracting out government functions. In some instances this had moved personal data outside the scope of federal privacy law. In addition, technology has raised the stakes, intervening in the relationship among Canadians, the private sector and government and permitting an unprecedented collection, use and disclosure of personal information.

Providing legal protection for personal information in the federally-regulated private sector is a goal that can be accomplished now. The ideal solution, of course, would be to have consistent privacy and data protection laws in the provinces and territories. Quebec already has put such legislation in place — the only North American jurisdiction to have done so.

A level playing field The discussion paper advocates harmonizing privacy and data protection laws in all Canadian jurisdictions. This is essential if the rules are to be consistent across the country and if we are to avoid building data havens — jurisdictions where less stringent laws could attract some businesses seeking to avoid their privacy obligations. Private sector legislation in the provinces should be modeled on the best features of federal private sector legislation, Quebec's private sector law, the Uniform Law Conference of Canada draft *Private Sector Protection of Personal Information Act*, and the Canadian Standards Association's Model Privacy Code.

Protection of personal information might also be considered a federal matter under the trade and commerce heading in the Constitution; this interpretation of the Constitution would enable the federal government to legislate uniform data protection across the entire private sector.

On the CSA Model The discussion paper highlights the work of the Canadian Standards Association (CSA) in bringing together representatives of the public sector, business, consumers and unions to draft a model code. The code establishes principles for private sector collection, use, disclosure and protection of personal data, as well as ensuring individual access to, and correction of, the information when necessary.

The Standards Council of Canada adopted the CSA code as a national standard in 1996.

Given the necessary teeth, the broad principles of the CSA Code provide a solid foundation for building privacy legislation. And the CSA Code has the added benefit of having won the endorsement of several provincial privacy commissioners. However, there remain a number of deficiencies that would result in a legislated data protection standard that is not sufficiently rigorous and would offer only the illusion of effective protection for personal information. For example, it is insufficient simply to identify the purposes for which personal information is collected. Individuals should also be told whether providing the information is obligatory or optional, the consequences of failing to provide the information, who will receive it and how they will use it.

Designing a new privacy law begs several questions about its administration and oversight. If it is to work, the law cannot be burdensome and bureaucratic for business. Nor can it impose on consumers an accountability process by exhaustion. The paper discusses several options.

Sectoral Codes & Registration While some countries require or encourage industry sectors to draw up more specific codes tailored to the demands of their industry and clients, we do not support codes as part of Canada's regulatory scheme.

While undoubtedly helpful to guide individual businesses, sectoral codes would be impractical. For a start, defining sectors would be difficult as industries continue to converge and re-align. It would also be difficult to ensure that the codes of each individual business were consistent with the sectoral standard. Finally, sectoral codes may be unnecessary. Quebec's private sector data protection law makes no use of sectoral codes and yet has not suffered since it came into force in January 1994.

Another feature of some national laws is the requirement that private businesses register their personal databases with a central authority. Registration would be unnecessarily costly and bureaucratic. It may also be a misapplication of resources that could better be used elsewhere to protect privacy interests.

Oversight Whatever the features of the law, it will need independent oversight; a body to review compliance and resolve disputes. The options range from requiring complainants to go to court — costly and burdensome for all parties (including the courts), to quasi-judicial tribunals, to data commissioners with order-making powers.

The ombudsman model, the scheme in place under the federal *Privacy Act*, offers the most effective approach. An ombudsman ensures administrative fairness using knowledge, impartiality and strong investigative powers. The essence of successful oversight is maximum reliance on consultation, conciliation and negotiation, and minimum resort to coercion and compulsion. The ombudsman's stick is the possibility of bad publicity — an effective tool if judiciously applied.

The Privacy Commissioner's oversight would entail promoting fair information practices, resolving complaints, and conducting audits. The Commissioner should also have the specific authority to identify and assess issues that may affect privacy — for example, workplace surveillance, personal identification technologies and the tracking of purchase information, even if these issues have not caused complaints. Given adequate infrastructure and resources, this office would be an effective oversight agency.

Extending the Privacy Commissioner's jurisdiction to the federally-regulated private sector would also be consistent with the scope of other federal oversight bodies such as the Office of the Commissioner of Official Languages.

Some business sectors suggested that oversight might be acceptable if conducted by existing regulators — such as the Superintendent of Financial Institutions for banks. However, this would lead to multiple regulators, without data protection experience, and inevitably result in uneven application, and thus uneven compliance with privacy standards.

Public Education No legislation will be effective without its being understood by public and business. Organizations and their respective associations should bear the primary responsibility for educating employees, management and the public. Informed consumers and employees are more likely to encourage organizations to adopt fair information practices. However, the proposed legislation should also

give the Commissioner a specific mandate and resources to increase public awareness about issues and new technologies that could affect privacy.

Complaints Process The complaints process must be administratively simple for both the complainant and the business which holds the personal information. Individuals should begin by trying to resolve their complaints directly with the organization. Since disputes often result from misunderstandings, many can be resolved at this stage. However, the organization should be free to refer the complaint directly to the Commissioner if it would prefer to have the complaint handled through the Commissioner's complaint resolution process. Time limits should be set for each stage in the resolution process to avoid unwarranted delays.

The Commissioner would make recommendations, as necessary, about the collection, retention, use or disclosure of personal information, as well as about any denial of access or correction. The Commissioner should further have the right to identify any appropriate redress for the complainant. The Office should be vested with powers to investigate and resolve complaints, such as those currently available under the federal *Privacy Act*.

The law should oblige the parties to participate in mediation facilitated by the Office. The Commissioner would then issue a non-binding evaluation of the parties' respective positions.

Compliance Audits The legislation should require organizations to undergo periodic information practices audits. The organization would be free to appoint the auditor of its choice and would be expected to take corrective action within a reasonable time after receiving the audit recommendations. In addition, legislation should authorize the Commissioner to conduct an issue-based audit of one or several organizations if the Commissioner has reasonable cause to suspect that their information handling practices are inadequate, or if the Commissioner receives multiple complaints about similar deficiencies.

Privacy Impact Assessments The Commissioner should provide organizations with the tools necessary to conduct privacy impact assessments on any activity that may affect privacy. This will help organizations avoid costly redesigns that may be necessary if fair information practices are not considered at the design phase of their activities. In addition, the Commissioner should have the authority to monitor disclosures for research and statistical purposes.

Protecting Health Information — Privacy under the weather

Last year's annual report spelled out the privacy implications of one aspect of the government's proposed national health strategy — a national health data network. We seem to have touched a nerve.

The loudest voices supporting the network are those seeking access to confidential medical records — for more efficient spending of limited health care dollars, improved flow of information between jurisdictions, and better evidence of what influences Canadians' health. All are worthy aims. However, making patient information available on-line (and integrating it with socio-economic data to create patient profiles) risks turning patient care into a “spectator sport”.

There are hopeful signs that others are listening. First, February's National Conference on Health Info-Structure brought together government representatives, health professionals, academics, consumers and business to develop action plans for establishing the info-structure. At the head of the list of policy issues discussed were “Privacy, security and confidentiality”.

In his opening remarks, Health Minister Allan Rock cited privacy as “perhaps the crucial issue. The credibility of a national strategy hinges on public confidence that privacy will be protected.” He acknowledged that many in the health sector were concerned that “stringent privacy rules could impose unreasonable limits on the information they need”, nevertheless he announced himself determined to see that Canadians “get the right protection for their most personal information”.

In the working session, other voices joined in to protest that effective and meaningful health care does not have to be compromised to protect patient privacy. However, network supporters argued that good security is the answer to real privacy protection. They urged that we build the systems first, then “fix” the privacy issue afterwards.

(At press time, there has been no public report of the conference proceedings or of any subsequent action plans.)

Developers of this network need reminding that using a patient's medical information without his or her knowledge and consent is an invasion of privacy, regardless of the system's security. That is the distinction between ensuring security and preserving privacy that must be maintained at all costs.

Medical information — and the circumstances under which much of it is provided — are unique. We are a captive audience when we are sick or hurt. At that vulnerable moment when we want our health restored, we feel compelled to provide intimate details of our lives we would otherwise choose to keep private. Health care providers need any and all personal information that might be helpful during a crisis. But this intimate information, once revealed, may become part of a “womb-to-tomb” electronic medical record.

At that point, the patient (and, arguably, the doctor) will have lost control. The details could become accessible far beyond the physician with whom the patient has established a trust relationship. Information could be shared with the broader health care system and perhaps also a present or future employer, an insurance company and the credit bureau. Information we volunteered for medical treatment could be used for unrelated purposes, with devastating effect.

There seems to be a view that a public health system justifies greater intrusions. As the links between life style, poverty and health become clearer, so grow the temptations to follow, assess, and then influence our choices so that we will not become a burden on the system. While understandable, this is the first step to a loss of autonomy. Making educated health decisions is one thing — being coerced quite another.

Canadian Medical Association Draft Code

Another encouraging sign is the Canadian Medical Association's draft Health Information Privacy Code, now being developed. The June 16 draft code meets the measures we set out in last year's report — and more. The added feature? While the CMA Code follows the general structure of the Canadian Standards Association Model Privacy Code, its content was inspired by the Parliamentary Committee's report, *Privacy: Where Do We Draw The Line*, which recognized privacy as a human right and social value.

In a background paper, the CMA recognizes that “initiatives advertised under the rubric of ‘protection of privacy’ often have less to do with privacy protection than with ensuring access for secondary use” and that “...[i]f ‘authorization’ is not in the hands of patients, then it is ‘doublespeak’ to say that ensuring access only as ‘authorized’ protects the right of privacy.”

The incentive for the CMA to promote privacy is obvious: ensuring the integrity of the doctor-patient relationship. Physicians swear in the Hippocratic Oath “what I may see or hear in the course of the treatment or even outside of the treatment in regard to the life of men, which on no account one must spread abroad, I will keep to myself holding such things shameful to be spoken about.” As the CMA paper observes “... [p]hysicians, in light of patients’ high level of trust and confidence in them, could therefore become unwitting instruments of betrayal. Behind physicians would stand any number of secondary users who are strangers to the patient-physician relationship but eager to share in information secured by physicians.”

As we go to press, the Code is expected to be presented to the CMA’s General Council for debate this September.

Investigations Branch

The record-setting complaint intake continues apace — 2,455, compared with 2,235 received last year. This increase is in keeping with the average growth of 10 per cent annually over the past ten years.

Staff completed 1,821 investigations, close to 900 fewer than last year. Last year's accomplishment was directly attributable to the Office's efforts to reduce a backlog of older complaints by streamlining the process, introducing a fast-track procedure for selected complaints, and using resources drawn temporarily from other parts of the organization. Those resources were not available this year.

For the past several years, the Office has first tinkered — then substantially revamped — its investigation process to eliminate bottlenecks and speed the process. However, more than tinkering is needed; as quickly as new approaches are tried, our clientele becomes more sophisticated and their complaints more complex. As the intake of new cases continues to grow, investigators are confronted with caseloads that are excessive, time consuming and unmanageable. The result for complainants is resolution delayed and, for investigators, burnout.

Coupled with this unmanageable caseload, increasingly investigators must deal with departmental privacy staff who are also overloaded and often impatient and uncooperative. Frustrated with repeated requests from some applicants who use the *Privacy Act* as a tool to conduct personal vendettas against selected departments, staff effectively stall investigators by rescheduling or delaying meetings, delaying identifying departmental contacts, or failing to produce the records for the investigator's review.

The Office is not unsympathetic to the departments' plight; some applicants do indeed make repeated requests that border on abuse of the system. They also make repeated complaints. However, the law makes no provision for either departments or the Commissioner to ignore or stall repeated requests or "trivial and vexatious" complaints. Nor does the Commissioner believe it should. The act obliges us to do our respective jobs; departments to respond in a timely manner and this Office to investigate any subsequent complaints.

The Commissioner cannot and will not tolerate departments stalling his investigators.

The open caseload at the end of the reporting year — 1780 — has also climbed from the 1147 open at the end of the previous year. One issue contributes 956 of these complaints; government's matching of Customs *Traveller Declaration Cards* with the Employment Insurance data base. This match is now before the Court (see page 89 for more detail).

Lingering investigations also contribute to some complainants' disappointment when the Commissioner concludes there has been no breach of the act. It is little consolation to someone who has waited months for the Commissioner's review only to be told that the department's actions did not offend their privacy rights. Some conclude that we have been of little help. In fact, the Office's rate of well-founded complaints, 48 per cent, is high compared with the traditional one-third ombudsmen's average.

The cases described below illustrate the type of concerns Canadians bring to the Commissioner.

Hosts tax documents not “required” for visitors visas

A journalist's question about Citizenship & Immigration demanding tax information from Canadian hosts before issuing a visa to their visitors, prompted an Ottawa couple to complain. The husband's sister was planning a business trip to the United States and wanted to spend a week with him in Canada.

When she applied for her visa to the Canadian High Commission in Colombo, Sri Lanka, they refused to process her application without an income tax document confirming the income of both the host and spouse for the last three years. The tax documents were “REQUIRED” (their emphasis). She was also asked who would pay for her trip to Canada.

The couple had provided proof of Canadian citizenship and their employment but objected to producing the income tax documents. According to C&I, before issuing visitors' visas, it wants to be sure that

the visitor will return home and not become a burden on Canadian society. The documents were meant to establish that the hosts could afford to support the visitor.

Apparently each high commission decides which documents visa applicants need, depending on local circumstances. The Columbo high commission began demanding a Revenue Canada Notice of Assessment in March 1997 to assess the financial situation of the hosts. They argued that bank statements and letters of employment are subject to abuse and inaccuracies, and are hard to verify. As well, affidavits simply cannot be enforced. The Notice of Assessment contains the taxpayer's amount of income and taxes paid and, since it is official, needs no further verification.

However, it was clear that tax documents were not essential to processing a visa application — although they could speed the process. High commission officials acknowledged that providing tax information is “voluntary” and have now emphasized this for all staff. At the Office's request, they have also amended the application form to remove the statement that the information is required.

The investigator asked C&I to determine what other embassies and high commissions ask on their visa applications. Of the 61 responses received, five showed tax information as “REQUIRED”. C&I agreed to contact each of the five and have them amend their forms.

It is questionable whether knowing someone's gross income helps assess his or her “financial situation”; some families live very comfortably on \$60,000 while others struggle with \$100,000. The complaint was well-founded and resolved.

Employee accesses woman's credit file

The notion that federal government departments have access to individual credit files is puzzling to many. The explanation is simple: many government positions have security requirements, ranging from the least demanding “enhanced reliability” up to various levels of Special Access reserved for highly sensitive intelligence work.

Employers check employees' credit references to ensure their finances are not in such a precarious state that they may be susceptible to financial "inducements" or blackmail. To prevent abuse, only a handful of departmental staff may have access to credit files — usually staff in the security units which are responsible for security clearances.

This restricted access sent alarm bells ringing when a woman complained that someone at a department where she neither worked or sought a job, had accessed her file at the local Ottawa credit bureau. Attached to her letter was a copy of her credit report listing those organizations which had obtained access. It included a departmental telephone number and the identification "Security Serv". The woman was going through a divorce and feared that her estranged husband, who worked in the department's Security Services, had queried her credit file.

Although the investigator confirmed at both the credit bureau and Security Services that the woman's file had been accessed, it was impossible to determine by whom. The department's credit checks are conducted by three employees, usually by computer-modem access using three telephone numbers. The same credit access password served all three computers and it was programmed into the automated query process. (Telephone queries require the caller's name which is recorded at the bureau.) During an internal investigation, staff found a hard copy of the woman's credit report in her husband's office, however it was in a different format from routine on-line queries.

The husband categorically denied having accessed his wife's file, arguing that he did not know how to conduct an on-line check and he believed he was at a regular Friday staff lunch when the query was made. The investigator's interviews with unit staff established that the husband's computer was not one of the three with access to credit files, that no-one had seen him at one of the terminals, nor had he asked them to conduct the check. However, the instructions for making an on-line query were readily available in employee in-baskets. A query to the government telephone system (GTIS) to establish precisely on which line the call was made came up empty because GTIS logs only long-distance not local calls.

The experience was a first for the department which has Privacy Directives available on every computer. The department responded by conducting its own internal investigation and tightening its credit access procedures. These include changing the system access code, introducing individual passwords for staff so that any future queries will identify the caller, and restricting access to the instructions for entering the system. It also reassigned the employee.

The Commissioner concluded that there was no doubt that the woman's credit file had been improperly accessed and that the complaint was well-founded. Although there was no remedy, the more stringent security measures should help prevent a recurrence. The Commissioner urges other security units to take note.

(Although the Office routinely identifies departments against which complaints are made, doing so in this case would effectively identify the individuals concerned, breaching the Commissioner's legal obligation to investigate in private.)

Commissioner's complaint tightens HRDC collection process

A provincial government manager alerted the Office to a Human Resources Development Canada (HRDC) collection which disturbed him. He had received more than a dozen requests from HRDC collection officers for information about former employees of his department and questioned their method of seeking the information, the amount of detail, and his obligation to respond.

Subsequently two federal government departments — Health Canada and National Archives — were faced with similar requests and also called the Office with concerns. Given the investigator's findings, these two were likely the tip of an iceberg. With sufficient information in hand, the Commissioner initiated his own complaint.

HRDC collection officers attempt to collect established overpayments of (un)Employment Insurance (EI). Approximately 80 per cent of the cases constitute fraud and some involve substantial sums of money. The EI legislation allows HRDC up to six years to recover the overpayment.

Although HRDC's demands for information varied from one city to another, most asked for the person's term of employment, reason for leaving, home address and telephone number, bank address, and name and address of current employer if known. HRDC officials in Winnipeg and Moncton also asked for the name and address of the person the former employee designated be called in cases of emergency.

The provincial manager had also received a request for detailed information about an individual's bank accounts and balances, RRSPs, GICs, term deposits, accounts at other branches and any company accounts. It was clear that this was an error since an employer would be unlikely to have such information. The request was intended for the employee's financial institution, not the employer.

The investigator sifted through all the information and allegations and focussed on six aspects of the case. An allegation that the requests were being faxed was found not to be true.

Had HRDC followed the proper procedure for collecting the information? The EI Act requires collection officers to request the information from any person "by notice served personally or by confirmed delivery service". This provides proof that any individual, employer or financial institution received the notice. It was evident that HRDC was not following the procedure because it was more expensive and more onerous than regular mail.

Could HRDC ask for names and addresses of emergency contacts? In effect, HRDC was seeking information about "unnamed persons" — information supplied for a specific and limited purpose about individuals who are not a party to the case. The EI Act stipulates that HRDC cannot require any third party to provide information about "unnamed persons" without a judge's authorization. This had not been obtained.

Can HRDC collect detailed financial information on clients from financial institutions? The broad authority to collect information from "any person" is clearly established in the EI Act. Having the financial details allows HRDC to seize financial assets once they mature — usually a last resort. Knowing account balances and other short term assets allows HRDC to calculate a repayment schedule or

the amount which could be garnished from the clients' pay (once they are located) without causing undue hardship. Apparently some financial institutions, which once routinely provided the information in response to mailed requests, have now begun questioning HRDC's requests for financial information.

Had collection staff cited the correct legal authority? Some letters (incorrectly) cited subsection 126(15) of the EI Act. This section deals with those unnamed persons and requires the judge's authorization. The correct citation is 126(14).

Were requests to federal departments flagged "protected"? Personal information in the hands of federal government departments must be labelled "protected" to help guard against unauthorized opening or access to personal data. The requests to Health Canada and National Archives were not properly flagged.

Why collect the reason for departure? If the employee worked for the government, HRDC can collect the debt by offsetting the amount against any severance, unused leave or pension payments.

Do collection officers have the authority to demand the information? The Employment Insurance Commission has the power to authorize "any person or body, or member of a class of persons or bodies" to exercise its powers. A list of those exercising delegated powers includes "Collection Officer, Overpayment Recovery". Clearly these staff have the authority to demand the information.

HRDC dealt with three of the four problems in a December 1997 memo from the chief of collection services. He reminded staff to deliver the letters personally or by confirmed delivery service; not to ask for the client's emergency contact without a judge's authorization, and to use the correct legal citation. HRDC staff are also reviewing the letters to attempt to standardize the language as much as possible, thus avoiding a repeat. They will also add a "protected" designation to help prevent unnecessary disclosures.

The Commissioner appreciates the department's ready cooperation and quick response to his recommendations to tighten the process.

Three-hour Family Expenditure Survey voluntary — next time

Statistics Canada surveys often cause ripples, particularly those dealing with individuals' finances. This year, a StatsCan decision to make one of its regular surveys compulsory prompted three complaints to the Commissioner and considerable public interest in British Columbia (but little elsewhere).

What distinguishes the Family Expenditure Survey (FAMEX) from many others the agency conducts is its length — almost three hours, the extent of the detail — 39 long pages, and its venue — the respondent's home. FAMEX examines household spending patterns and gathers information on their income, assets, debts, occupation and education.

One complainant described the survey as “grossly intrusive”. He questioned whether StatsCan had the authority to compel responses and observed that the detail demanded was far beyond the scope required for the Consumer Price Index. Two questions cited in the ensuing publicity were those asking for “...sanitary and incontinence supplies...” and “condoms, syringes, etc.”. (In fact, these products — while unfortunate choices — were simply examples to illustrate the types of expenses in the respective categories.)

The complainant also argued that it was both a “conflict of interest and a gross abuse of power to compel by law an individual (to) provide this information, then market it for business to use in developing their own markets”.

StatsCan uses some of the information to update the Consumer Price Index, a shopping basket of some 600 goods and services it tracks to measure inflation. The data can lead to changing the items in the basket or altering their relative weight in the total cost. Government can also use the data to relate people's spending patterns to their age, family size and income. These factors influence policy on welfare reform, wage settlements and support payments. The results also help government compare living costs and standards between various regions, and between Canada and other countries.

However, there is no doubt that the information is sold. In its promotional material to business, StatsCan extols its ability to tailor the data

from FAMEX “to meet your specific needs”. The data is not personal, of course, but “can be cross-referenced by household income, metropolitan area, age, dwelling owned or rented, household composition, or other selected household segments”. This allows business to target its marketing to appropriate groups.

Responding to all StatsCan surveys is compulsory unless the Minister decides otherwise. The *Statistics Act* imposes penalties on those who refuse although StatsCan is loath to be heavy-handed. Regular FAMEX surveys began in 1952. Participation became voluntary in 1984, then reverted to compulsory in 1996 when StatsCan felt that the response rate, which had dropped to 74 per cent, was too low.

The 1996 survey selected 16,000 households across the country in proportion to population. The already lengthy survey could take even longer for those with higher incomes if they have a greater range of expenditures and more complex finances. The survey questions are divided in broad categories of expenditures on

- housing, equipment, furnishings and services
- groceries, alcoholic beverages and restaurant meals
- clothing
- personal care products and services
- dental and medical products and services
- vehicles and expenses
- recreational products and expenses
- personal income and investments

The level of detail is intense: house furnishings includes such purchases as “sheets and pillowcases” and “plastic garbage bags”; health care details include “e.g. first aid kits, bandages, condoms, syringes etc.” and “razors and razor blades”; women’s clothing includes “lingerie”; recreational expenses seeks “photographic film, processing, extra prints and enlargements”; reading materials wants “paperbacks and pamphlets”, the income category asks for the value of gifts received from non-family members.

One might well wonder how many Canadians could possibly recall these expenditure details a year later, nevertheless the expansive language of the *Statistics Act* gives StatsCan the power to compel responses. The investigator had to quickly disabuse the complainants of any notion that the Commissioner could exempt them from responding. However, there were aspects of the process which need clarifying, primarily concerning its transparency.

First was the assertion that the survey had to be conducted in the form of an interview. This requires respondents to furnish personal details to a stranger rather than simply complete a form on their own time. StatsCan clearly prefers personal interviews to clarify questions, prompt responses and ensure the form is completed. It is also concerned about the quality of the data. However, simply completing the questionnaire meets both the respondent's legal requirements and StatsCan's needs. Individuals who feel competent to do so on their own, should be offered that option at the outset.

A second concern was an apparent requirement that the interview take place at home. Letters alerting local police, politicians and residential property managers to the survey (in case of calls) make it clear that interviewers "will visit their (respondent's) home to conduct the interview". However, the advance letter to the respondent is less forthright — the "interviewer will visit you to enlist your support in this important study".

Being subjected to such detailed questions in one's own home can seem very intrusive. Although StatsCan interviewers would be prepared to meet respondents elsewhere, it argues that most people would need their records to complete the survey and clearly prefers, and "sells", the in-home interview. Nevertheless, respondents are clearly not compelled to agree.

Respondents can take some comfort in knowing that the interviewers undergo an "Enhanced Reliability Check" (which includes a criminal history check) and are subject to the same legal obligations as all StatsCan employees. They carry identity which can be verified by calling a telephone number supplied.

The individuals' identity is not entered into the data base and the data is encrypted before transmission to Ottawa. At that point, the paper questionnaires are sent for archiving where staff detach the householder information. The only link between paper and data is an identifying number on the questionnaire which could be linked back to the paper responses. However, StatsCan has no interest in identifying respondents, except for data verification.

Making the survey mandatory achieved the desired objective of increasing participation (the rate rose by about 12 per cent) but may have affected the statistical accuracy by encouraging some unhappy respondents to be less than candid (or thorough). StatsCan has decided to return to voluntary participation for the next survey and to compensate by increasing the sample size to 27,000.

Unfortunately the informational material for the new Survey of Household Spending is less than forthright on the legal options available to selected respondents. The notification letter advises that the interviewer "will visit you" and asks for "your support in completing a questionnaire" but does not explain that participation is voluntary. An accompanying brochure acknowledges "while your participation is voluntary, it is important for all selected households to participate...". It continues assuming that "the interviewer comes to your home..." and that "the interviewer will go through the questionnaire with you". No alternatives are offered.

The Commissioner concluded that while Statistics Canada undoubtedly has the legal authority to conduct the FAMEX survey, it had not been frank with respondents about why it was collecting the information and how it would be used. On that basis he considered the complaint well-founded.

No tax information without the taxpayer's consent

The introduction of new seniors benefit plans in Alberta and Ontario led to a number of complaints that the federal government was disclosing individuals' income tax information to the provincial organizations administering the plans. Since the benefits of both plans are linked to income, the provincial bodies wanted confirmation of the applicant's income — the most dependable source being income tax files.

Revenue Canada enters agreements with provincial government organizations to provide specified tax information — but only with the taxpayer's consent. Among the issues raised by these complaints was

- Did the applicants consent?
- Was Revenue Canada the source of the information?
- Were any disclosure kept to the minimum necessary to meet the programs' goals?

The Alberta Seniors Benefit Program

This program entitles low-income seniors to certain financial benefits. However, to qualify the senior must establish that their income is below the level set by the Alberta Ministry of Community Development (ACD) which administers the program.

In an October 1994 Memorandum of Understanding, Revenue Canada and ACD agreed to "large volume transfers of taxpayer information in electronic media" on condition that ACD obtained taxpayers' "proper written authorization". Applicants were asked to sign a consent clause authorizing Revenue Canada's disclosure to ACD. ACD kept the forms and, using seniors' Social Insurance Numbers, submitted a bulk request to Revenue Canada beginning in November 1994.

Unfortunately, ACD did not check that all consent clauses were signed and simply submitted the entire list of applicants to Revenue Canada. Among the 60,000 of the 194,000 total applications checked, 4,000 lacked completed consents — and 12 contained outright refusals, several of whom complained to Alberta Privacy Commissioner Bob Clarke. Given the implications for so many seniors, the complaints were merged into a general complaint sponsored by the Alberta Council on Aging to both the provincial and federal privacy commissioners.

The two commissioners followed the trail from each end of their respective jurisdictions and met in the middle. Mr. Clarke examined ACD's collection of the forms and request to Revenue Canada. This Office investigated whether Revenue Canada disclosed tax information without consent; whether it disclosed more information than was required, and whether the original authorization form for Revenue Canada's disclosure to ACD met the requirements of the *Privacy Act*.

The federal investigator found that the first condition of the federal/provincial understanding was not met; ACD did not get proper taxpayer authorization before seeking the information from Revenue Canada. Revenue Canada assumed that all individuals on the ACD list had consented and replied with a standardized printout on everyone, containing 75 fields of data. It was evident that Revenue Canada had disclosed the information improperly, albeit on the assumption that ACD had kept its part of the bargain.

However, it was also obvious that Revenue Canada had disclosed far more information than was needed to confirm the taxpayers' income — 75 lines of information rather than 12. The 75 lines include detailed breakdowns of income sources and exemptions (including alimony, charitable donations and medical expenses).

The investigator was able to dispel suspicions that Revenue Canada was also disclosing “T-slip” information about non-filers to ACD. T-slips are statements of income sent to Revenue Canada about individuals who may not file a return; for example, a bank reporting a small amount of interest on a savings account.

The complaint investigation led ACD to purge the 1993 and 1994 tax information from its files and to first freeze, and then destroy, 1995 data in December 1997. Revenue Canada now supplies just the minimum required data, and routinely audits selected individual's files to ensure they consented.

The Commissioner considered well-founded the complaints of improper disclosure against Revenue Canada but by destroying the data, amending the memorandum of understanding, restricting the amount of future disclosures, and conducting regular audits of consent forms, the department had acted effectively to prevent a recurrence. He dismissed the complaint that the ACD form was not a valid consent under the *Privacy Act*.

The Ontario Drug Benefit Plan

Following introduction of the plan which subsidizes drug costs for low-income seniors, the Commissioner received 25 complaints about the federal government disclosing income information to the Ontario government — and through the computer system — to pharmacists filling seniors' prescriptions. Some complainants cited Revenue

Canada; others, Human Resources Development Canada (HRDC). The investigator quickly determined that Revenue Canada had been approached by the Ontario government but refused to provide individuals' tax data unless they consented. The focus then turned to HRDC.

Income information became critical when the new plan took effect in July 1996. Now single seniors with incomes less than \$16,018, and married seniors with incomes under \$24,175, must pay a \$2 dispensing fee. Those with higher incomes pay the first \$100 each year, then a \$6.11 dispensing fee for each subsequent prescription.

HRDC obtains income information when individual seniors apply for the federal Guaranteed Income Supplement or Spouse's Allowance. Because these benefits are linked to income, the application form asks for the senior's income and indicates that it will be verified with Revenue Canada under an information sharing agreement. The match is not described in *Info Source* — as the government data matching policy requires — or in the program's information brochures. *Info Source* does describe sharing information with the provinces as a "consistent use".

HRDC has provided the Ontario Ministry of Finance with monthly computer tapes of Guaranteed Income Supplement recipients since 1975 under a sharing agreement to administer the provincial Guaranteed Annual Income Supplement (GAINS). These agreements are allowed under the *Old Age Security Act* to administer social, income assistance and health insurance programs. However, the agreement stipulated that the information would be used only for GAINS. The following year it was amended to allow the Ontario Ministry of Revenue to share the information with the provincial health ministry to issue an OHIP card entitling seniors to free drugs.

At some point, for convenience, HRDC began sending separate tapes to the Ministry of Finance for GAINS, and to the Ministry of Health for OHIP. Since the drug card was available to all seniors, the OHIP tape included all Old Age Security recipients, not just low-income seniors, and contained new fields including date of birth, sex, language, SIN, dates of any deaths, and the amounts of both OAS and any supplements received for the current year. No other income information was provided.

Then, in January 1996, the Ontario Ministry of Finance asked HRDC whether the 1976 agreement would cover information sharing for the new income-linked drug plan. HRDC responded that the information could be used for the purposes specified in the original agreement. The Ontario Health Ministry concluded that the purpose was the same and used the OHIP tape to establish the drug benefit program. In August 1996, HRDC determined that the existing sharing agreement did not authorize the new use.

A series of meetings ensued to consider a new agreement, then were suspended until the parties could agree specifically what information the province needed to administer the new program. It was evident that a new agreement would have been essential to launch an income-linked program had HRDC not been routinely sending OAS and GIS payments information to OHIP. Without this information, OHIP could not have determined definitively who met the income test.

It was also evident that HRDC had been regularly disclosing unneeded benefit information and that seniors had not been told.

Resolution of the complaints led HRDC to stop sending OAS information to the Ministry of Health, to rescind the 1976 sharing agreement allowing the Ontario Ministry of Finance to disclose information to the Ministry of Health, and to amend the OAS/GIS forms and explanatory material to make it clear to applicants that information is shared with the province.

The complainants were particularly concerned about pharmacists knowing their income in order to bill the correct amount. Although pharmacies are not subject to federal (or indeed any) privacy law, the investigator asked a local pharmacist for a demonstration of the on-line billing system.

This pharmacist registered all clients into his/her computer system. When a senior filled a prescription, the pharmacist identified the client, entered the flat \$6.10 fee and the cost of the drug and transmitted the information to the ODBP data base. ODBP responded with confirmation of the amount the customer is to pay; either the full cost of the prescription, the \$6.10 fee if the \$100 limit has been reached, or the subsidized \$2.00 fee. While the pharmacist can infer the senior's income from the fee charged, there is no disclosure of specific income.

Revenue Canada shares some tax data for B.C. Family Bonus

Financial information — particularly income tax data — is very sensitive. Any suspicion that Revenue Canada may be sharing tax information prompts complaints, even when the recipient is a provincial government.

One Revenue Canada disclosure led a member of Parliament to complain on his own and a constituent's behalf. Revenue Canada was alleged to have shared individuals' income tax data with British Columbia to determine who was eligible for the B.C. Family Bonus.

The plan, which is income linked, is designed to help low income families with child-rearing costs. B.C. residents are notified that they do not have to apply for the bonus "as it is sent automatically based on the family's yearly income tax return".

Revenue Canada administers income tax for all provinces (except Quebec) under agreements between the provinces and the federal Department of Finance. It also administers the B.C. family bonus entirely, identifying qualifying families from family income and a pre-determined formula and mailing out the monthly cheques. It notifies the Department of Finance of the total amount which is then deducted from the provincial share of taxes remitted to the B.C. Department of Finance. Finally, Revenue Canada sends recipients' names and addresses to the B.C. government which, in turn, sends out notices to qualifying families so as to gain provincial visibility for the program.

The limited sharing of information took place under an interim agreement while a permanent Memorandum of Understanding was being drafted. The *Income Tax Act* allows Revenue Canada to disclose taxpayer information to a province "to administer a law of a province for which it can collect taxes" and to officials "of a province entitled to receive a payment". The *Privacy Act* specifically allows this type of sharing "under an agreement or arrangement between the Government of Canada and the government of a province" (sub-section 8(2)(f)). As well, it allows disclosures permitted in any other Act of Parliament.

The Commissioner concluded that the information sharing was permissible and the complaint not well-founded.

Names and addresses not disclosed to mail order drug firms

Late in 1995, personally addressed solicitations from a mail order pharmacy began arriving in the mailboxes of many public servants. The letters from MEDITrust or (in Quebec) La Pharmacie MARCEL Dubuc announced their agreement with the federal public service health care plan to supply prescription medications to members by mail.

During the following weeks, 65 employees complained to the Commissioner that someone had disclosed their names, addresses and public service status to the companies — their suspicions focused on their individual employers.

The investigation revealed that in August 1991, the National Joint Council (representing management and public service unions) recommended changes to the employees' health plan to make it self-insured. The Treasury Board (the public service employer) awarded the contract for the new plan to Mutual Life Assurance Company. In an attempt to control costs, the Council opted to use a mail order pharmacy to lower dispensing fees and medication prices. The successful bidders for the contract were MEDITrust and La Pharmacie MARCEL Dubuc.

In order to inform members of the new service, the Council asked the pharmacies to provide literature and blank envelopes to Mutual Life and the public service unions. The unions then mailed the literature to their members, and Mutual Life to members who had submitted medical claims since it took over the plan.

The Commissioner was satisfied that there had been no improper disclosure because employees' names and addresses were not given to the pharmacies. However, he was concerned that the old health plan contract contained no privacy protection clauses. With the contract under review again, he asked Treasury Board to incorporate clauses dealing with government control and individual access to the medical data.

Over several months, while the investigator pursued the contract provisions with the Treasury Board, the Council began reviewing its support of the mail order pharmacy. In March 1997, the Council advised members that “only a small number of plan members chose to enrol” and

thus the hoped-for savings had not materialized. Apparently the Council had not anticipated such a negative reaction to the use of mail order pharmacies. The plan was discontinued.

Progress on the contract provisions was slow because Treasury Board staff were not convinced that privacy clauses were needed. As well, the new health plan provider, Sun Life Insurance Company of Canada, had not factored in any costs to put the clauses in place.

Asked to review the proposed clauses the following summer, Office staff suggested that since Sun Life was a signatory to the Privacy Guidelines of the Canadian Life and Health Insurance Association, it use that model for the contract clauses. Ultimately, the contract signed in the fall of 1997 bound Sun Life to the Canadian Standards Association Privacy Code. The code gives individuals access to their plan records and limits disclosures of personal information to the employer (except for legal action, fraud or audit).

Parks Canada plays nanny

An Alberta woman complained to the Commissioner that Parks Canada (part of Canadian Heritage) had her supervisor monitor her comings and goings while she was on unpaid leave to care for her child.

Notes on her whereabouts, including her visits to the supervisor's neighbour, a museum and a local gas station — and observing whether the child was with her — were found in the work diary of the woman's supervisor. Apparently a human resources manager had instructed the supervisor to record the details because the woman was a "problem employee".

The information came to light in the department's response to a comprehensive and formal privacy request the woman filed at the privacy investigator's suggestion. Several earlier informal requests to see her personal files had not turned up several documents she believed existed.

Why the woman's behaviour needed documenting was a puzzle. "Leave without pay" is granted under the public service collective agreement

and cannot be refused. Employees' jobs are not kept open during this type of leave (they have priority for available jobs should they choose to return to work). Parks Canada maintained that since it had granted the woman "care and nurturing" leave, it was responsible for ensuring that she was indeed looking after her child — an extraordinary incursion into an employee's private life.

There is no conceivable reason for an employer to be concerned with an employee's daily routine while on unpaid leave because there can be no "abuse" of the leave. Even surveillance of current paid employees would need to meet the most stringent tests — employers should have no right to dictate how employees live their private lives.

The Commissioner described the diary entries as "a form of surveillance" which the department had no justification for conducting. The complaint was well-founded.

The department agreed to remove and destroy the information in the administrative files as part of its resolution of the woman's grievance. However, officials resisted the Office's request to also remove the material from its privacy unit files, arguing that it should be kept for at least two years after the last administrative action which was resolving her complaint.

This two year minimum is designed to allow individuals a reasonable time to access personal information in government records. Since the information should not have been collected, and the complainant has seen it and wanted it destroyed, the Commissioner urged the department to grant her request. The department eventually agreed and the Commissioner considered the matter resolved.

Video surveillance "excessively intrusive" — and unjustified

Of all the tools in an employer's arsenal, covert surveillance of its employees is surely one of the most intrusive and thus should meet the most rigorous tests. A complaint against the Immigration Refugee Board (IRB) illustrates.

A lawyer representing a refugee applicant told the IRB that within hours of her client's *in camera* hearing, a third party told the refugee

that her application had been approved. According to the refugee, the third party had been seen in the company of an IRB employee whom she described. The lawyer complained to IRB.

Concerned about the leak of information and a possible internal source, Board security staff began an internal investigation. Security staff focused on the employee based on the refugee's description which appeared to match the employee — a clerk in one of the regional offices. IRB senior management approved the use of a camera which remained in place until a Public Works technician moved some ceiling tiles during routine maintenance and dislodged it in the employee's presence. IRB then removed it.

The Commissioner concluded that the Board's evidence was insufficient to warrant such excessively intrusive surveillance; it amounted to hearsay and the employee's acquaintance with the third party. The investigator determined that security staff had never considered confronting or consulting the employee. As well, using a video camera (without audio capability) trained on the clerk's desk begs the question of what useful information it could possibly have captured. Presumably an employee leaking information would not do so in the middle of the employer's premises in full sight of everyone. And, without audio, the camera would not capture compromising phone calls.

The Commissioner questioned the Board's resorting to covert surveillance on mere suspicion. "In my view, surveillance should only be carried out after conducting a thorough preliminary investigation that would lead an employer to have reasonable cause to suspect an employee of wrongdoing, and only after all other investigative techniques have been exhausted or considered to be ineffective" he wrote. He asked for the Board's representations.

The Board responded, acknowledging that "in hindsight, an investigation by a law enforcement agency would have been preferable". The Board had apologized to the employee and drafted a policy to guide staff in any future incidents. While the Commissioner applauded the intent, he had several recommendations on the specifics. (See below.)

The Commissioner concluded that although the Board had reason to be concerned about leaks, and an obligation to protect personal infor-

mation, its investigation method was excessive given the dearth of evidence. He considered the complaint well-founded.

Needed: A government policy on employee surveillance

Not content to leave the matter there, the Commissioner wrote to the Treasury Board urging it to draft a government-wide policy on covert employee surveillance. As a foundation, he offered the recommendations made to IRB.

His recommendations were both general — concerning any investigation of employees — and specific. Any policy on covert video surveillance should satisfy *all* the following requirements:

- reasonable grounds to suspect serious misconduct, which may include criminal misconduct, must exist before covert video surveillance is considered an investigative option;
- use only when all other reasonable measures, including non-investigative measures such as counselling, workplace notices and education programs, have proven ineffective or are likely to prove ineffective;
- do not use where individuals have a reasonable expectation of privacy (for example, change rooms). If the alleged conduct under investigation is believed to be criminal, police should be asked to investigate. This will ensure a court review since police must first obtain a warrant to conduct covert video surveillance where there is a reasonable expectation of privacy;
- where individuals do not have a reasonable expectation of privacy, authority to order covert video surveillance should rest only with the head of the government institution personally, and not be delegated;
- to the extent possible, covert video surveillance should not intrude on the privacy of persons other than the individual under investigation;
- the surveillance must not continue longer than is reasonably necessary to conduct the investigation;

- access to the videotape and any information generated by the videotape must be strictly limited to those who have a legitimate investigative need for the information, and must not be used, for example, as a vehicle for monitoring employee performance generally; and,
- the individual placed under covert video surveillance must be notified afterwards about the surveillance, including where and when it occurred, and the justification for the surveillance, unless there are compelling reasons not to do so.

Using postcards risks immigration disclosures

Like anyone else faced with workload volume and time limits, public servants look for faster and more efficient ways of doing business. All to the good providing individuals rights are respected. However, when the Canadian Consulate in Buffalo, N.Y. began acknowledging immigration applications on an open postcard rather than in a sealed envelope, a Toronto consultant complained that using postcards effectively disclosed that the person was an applicant.

The investigator found that the Buffalo consulate was temporarily snowed under with 5000 immigration applications. The sudden influx was caused by applicants trying to have their cases locked in under old regulations before the new ones took effect on May 1, 1997. The Buffalo office is the only mission in the United States which can accept immigration applications.

To acknowledge the applications quickly, the consulate had resorted to cards on the face of which appeared the applicant's name, file number and the notation that the individual's "application for permanent residence has been received".

Citizenship and Immigration headquarters alerted both the Buffalo consulate and all missions abroad that open cards risk improper disclosures of personal information. The consulate switched back to sealed form letters and the complainant was satisfied. The complaint was considered resolved during investigation.

CRTC refers cable billing complaints to industry council

Many Canadians are under the impression that complaints about broadcast content and cable billing are the turf of the Canadian Radio-Television & Telecommunications Commission (CRTC). Not so. The misunderstanding led a Toronto man to complain that the CRTC had improperly disclosed his complaint about a local cable supplier to the Cable Television Standards Council, and to the cable company.

As part of its 1988 regulatory reform, the CRTC encouraged the broadcasting industry to assume responsibility for dealing with disputes over such issues as subliminal and sexist advertising, violence, content of children's programming and lotteries. The cable sector was also to deal with billing and service complaints.

Broadcasting sectors were asked to develop industry standards and submit these for CRTC acceptance. Compliance with the standards and complaint resolution is overseen by industry councils for each sector — in the case of cable TV, the Cable Television Standards Council (CTSC).

The man's complaint to the CRTC about billing irregularities and rude treatment by company staff was forwarded to the council which, in turn, sent it to the cable company. The company is required to respond in writing and, if its response is unsatisfactory, the complainant can take the matter to the council. Member cable companies are bound by council decisions.

Given the new scheme, the disclosure allowed the company to respond and the council to see that the problems were resolved. The complaint was not well-founded. Although the man was satisfied with the investigator's explanations, he continued to be upset that neither the CRTC or the council had followed up with him. The CRTC considers billing arrangements a matter between subscriber and cable company and closed its file.

New personnel numbers will end disclosure of SINs to union

Another complaint about the ubiquitous number concerned Canada Post's disclosure of employees' SINs to the Canadian Union of Postal Workers (CUPW). The employee's union membership card displayed his SIN and it had also been given to an insurance company.

The investigator established quickly that Canada Post had disclosed the information and was simply complying with the terms of its collective agreement with CUPW. Canada Post's payroll system uses SINs and the union argues that it needs to identify its members in the system. As well, members in good standing are covered by an insurance policy held by the union, and can buy additional coverage. Since administration of this coverage is also tied into the Canada Post payroll system, CUPW gives members' SINs to the insurance company.

The Public Service Staff Relations Board has ruled on several occasions that employees' SINs must be provided to unions, despite the restrictions in the *Privacy Act*. Nevertheless, the Commissioner is concerned about the practice and encouraged the Department of Justice to appeal one of the cases. In the meantime, Canada Post is converting to a Human Resources Identification Number to replace the SIN. The conversion was on hold at that point as Canada Post prepared for the strike. Once completed, disclosures of SIN will end.

Any question about union or insurance company use of the numbers is outside of the Commissioner's jurisdiction.

Inquiries

Inquiries are all those calls and letters which do not fit the definition of “complaints” to the Privacy Commissioner. Inquiries can include requests for general information and publications about the act, complaints about organizations not covered by the Act — Crown corporations, provincial and municipal governments or the private sector — and privacy issues beyond protecting personal information.

This past year, the two inquiries officers handled 10,331 requests on everything from access to adoption records, to disclosure of credit and financial information, and use of surveillance cameras on street corners. Many calls dealt with questions surrounding the matching of Canada Customs’ *Travellers Declaration Cards* with Employment Insurance data, some of them seeking advice on handling appearances before Boards of Referees and Umpires. While the Office cannot give legal advice to individuals caught up in the process, staff did provide callers copies of a letter setting out the Commissioner’s position on the match.

The mailing of the B.C. Benefits consent letter with its comprehensive collection statement (see page 82) flooded the telephone lines with calls, some of them seeking the federal commissioner’s intervention to effectively “overrule” the provincial government. Of course, the federal commissioner has no jurisdiction in provincial matters and referred calls to both the provincial privacy commissioner and the caller’s MLA.

The Toronto Dominion Bank’s new privacy brochure also moved many to call, objecting to the bank’s requirement that customers opt out of its plans to share information with subsidiaries. Customers had until October 1997 to indicate their preference. No news meant the information would be shared. While privacy advocates prefer active over passive consent, opting out meets the consent test set out in the Canadian Bankers Association Privacy Code, and the Canadian Standards Association Code on which it is modelled.

Inquiries officers have been enlisted in the Office’s quest to deal with some matters quickly and informally, whenever possible. In one case an MP’s office called to alert the Commissioner that Human Resources Centres in Newfoundland were asking EI claimants picking up cheques during the postal strike, to sign a receipt which listed all

claimants and the amounts of the cheques. Everyone picking up a cheque could see who else was drawing EI and how much.

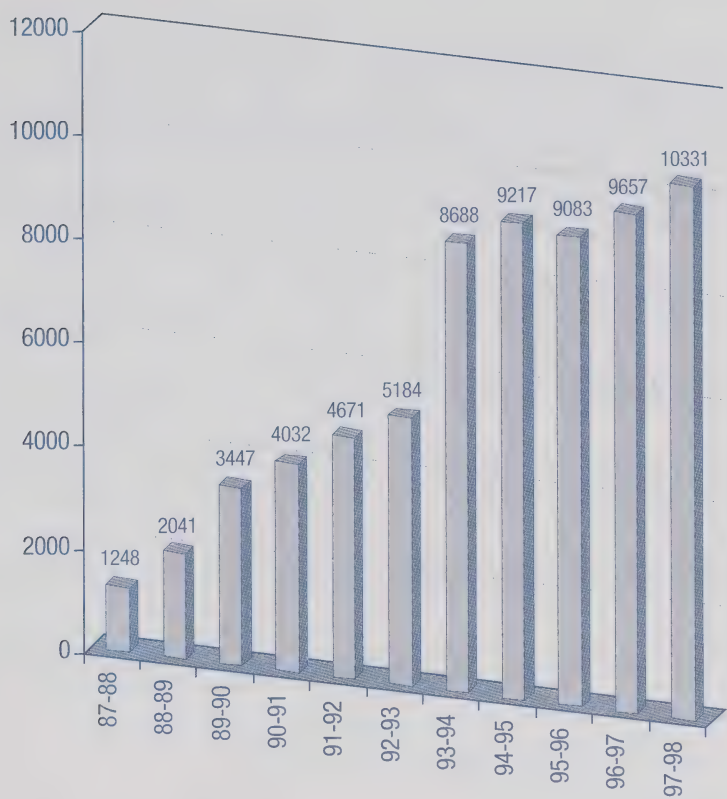
The inquiries officer confirmed the story with HRDC staff and asked them to intervene quickly. Apparently the practice was confined to Newfoundland and the Windsor, Ontario area. HRDC headquarters staff alerted the regions which switched to individual receipts, the practice in the rest of the country. The problem was resolved the following day.

Inquiries by type

The following table breaks down the inquiries into broad categories.

Privacy Act, interpretation & process	4,812
No jurisdiction, federal	358
No jurisdiction, private sector	401
Redirect to provincial commissioner	810
Redirect to other federal agency	270
Redirect to other	74
Social Insurance Numbers	523
Financial inst., insurance, credit	327
Telecommunications	100
Telemarketing, direct mail	42
Criminal records, pardons, U.S. waivers	154
Medical	120
Adoption, genealogy, missing persons	97
Other	726
Public affairs (media, publications)	1,517
TOTAL	10,331

Inquiries 1987-98



Top Ten Departments by Complaints Received

		Grounds		
Institution	TOTAL	Access	Time	Privacy
Human Resources Development Cda.	781	69	41	671
Revenue Canada	572	71	145	356
National Defence	336	84	233	19
Correctional Service Canada	263	123	98	42
Royal Canadian Mounted Police	95	65	10	20
Citizenship and Immigration Canada	69	30	28	11
Justice Canada	59	34	22	3
Canadian Security Intelligence Service	31	31	0	0
Canada Post Corporation	27	15	3	9
National Parole Board	24	12	6	6
OTHER	195	95	50	50
	TOTAL	2452	629	1187

Completed Investigations by Grounds and Results

Grounds	Disposition						TOTAL
	Well-founded	Well-founded; Resolved	Not Well-founded	Discontinued	Resolved	Settled	
Access	20	99	288	60	51	217	735
Access	19	94	267	60	51	210	701
Correction/Notation	1	4	20	0	0	6	31
Inappropriate Fees	0	0	0	0	0	1	1
Index	0	0	0	0	0	0	0
Language	0	1	1	0	0	0	2
Privacy	28	27	217	44	24	81	421
Collection	2	8	35	4	10	20	79
Retention & Disposal	6	0	12	7	0	8	33
Use & Disclosure	20	19	170	33	14	53	309
Time Limits	590	0	42	24	1	13	670
Correction/Time	31	0	1	1	1	0	34
Time Limits	559	0	29	22	0	13	623
Extension Notice	0	0	12	1	0	0	13
TOTAL	638	126	547	128	76	311	1826

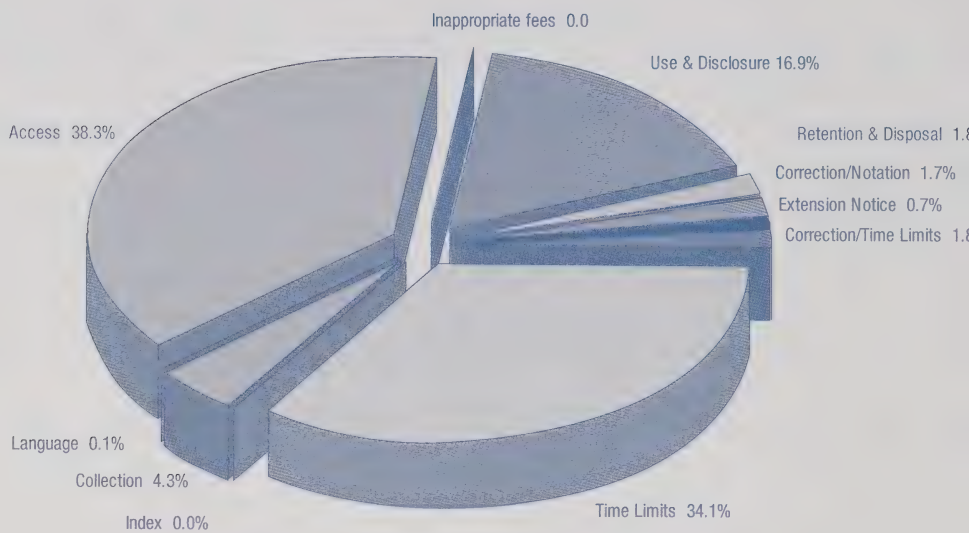
Completed Investigations by Department and Result

Department	Total	Well-founded	Well-founded; Resolved	Not well-founded	Discontinued	Resolved	Settled
Agriculture and Agri-Food Canada	4	1	2	1	0	0	0
Auditor General of Canada	1	0	0	0	1	0	0
Bank of Canada	4	0	2	1	0	0	1
Business Development Bank of Canada	2	0	2	0	0	0	0
Canada Deposit Insurance	1	0	0	0	0	0	1
Canada Mortgage and Housing Corporation	2	0	1	1	0	0	0
Canada Ports Corporation	3	0	0	0	0	0	3
Canada Post Corporation	53	0	4	23	4	0	22
Canadian Heritage, Department of	9	1	2	3	2	0	1
Canadian Human Rights Commission	3	0	0	2	0	0	1
Canadian International Dev. Agency	6	1	1	3	0	0	1
Canadian Radio-Television and Telecommunication Commission	4	0	0	4	0	0	0
Canadian Security Intelligence Service	51	0	0	44	0	0	7
Canadian Space Agency	1	0	0	1	0	0	0
Citizenship and Immigration Canada	95	28	41	9	5	0	12
Commissioner of Official Languages	2	0	1	1	0	0	0
Correctional Investigator of Canada	1	0	0	1	0	0	0
Correctional Service Canada	373	124	24	109	33	25	58
Elections Canada	2	1	0	0	0	0	1
Environment Canada	6	3	0	3	0	0	0
Farm Credit Corporation Canada	2	0	1	0	0	0	1
Fisheries and Oceans	2	0	0	1	0	0	1
Foreign Affairs and Int. Trade Canada	16	4	0	5	4	1	2
Health Canada	9	2	0	4	2	1	0
Human Resources Development Canada	157	42	13	43	4	7	48
Immigration and Refugee Board	58	9	5	18	7	7	12
Indian and Northern Affairs Canada	8	4	1	0	0	0	3
Industry Canada	8	1	1	1	0	1	4

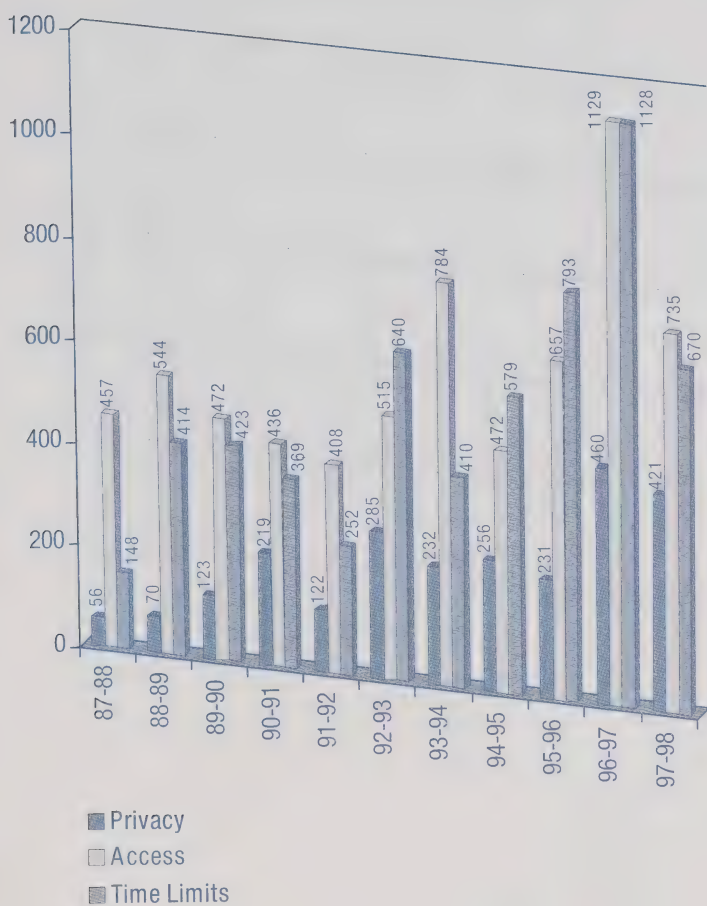
Completed Investigations by Department and Result (cont'd)

Department	Total	Well- founded	Well- founded; Resolved	Not well- founded	Discon- tinued	Resolved	Settled
Jacques-Cartier & Champlain Bridges Inc.	2	0	0	2	0	0	0
Justice Canada, Department of	40	12	6	8	4	2	8
National Archives of Canada	20	7	1	6	0	1	5
National Defence	300	220	4	16	14	4	42
National Library of Canada	2	0	0	0	0	0	2
National Parole Board	30	2	6	11	5	2	4
National Research Council Canada	1	0	0	0	0	1	0
Natural Resources Canada	4	0	1	0	0	0	3
Office of the Superintendent of Financial Institutions	2	0	0	2	0	0	0
Privy Council Office	7	2	0	2	0	0	3
Public Service Commission of Canada	10	6	0	2	1	1	0
Public Service Staff Relations Board	2	0	0	0	0	0	2
Public Works and Govt. Services Canada	13	0	3	7	0	0	3
RCMP Public Complaints Commission	4	0	0	2	1	0	1
Revenue Canada - Customs, Excise and Taxation	293	156	1	65	28	15	28
Royal Canadian Mounted Police	109	6	2	64	10	4	23
Solicitor General Canada	4	2	0	1	0	1	0
St. Lawrence Seaway, The	1	0	1	0	0	0	0
Statistics Canada	3	0	0	0	1	0	2
The Canadian Wheat Board	3	0	0	3	0	0	0
Transport Canada	15	0	0	8	0	3	4
Treasury Board of Canada Secretariat	70	2	0	66	1	0	1
Veterans Affairs Canada	8	2	0	4	1	0	1
TOTAL	1826	638	126	547	128	76	311

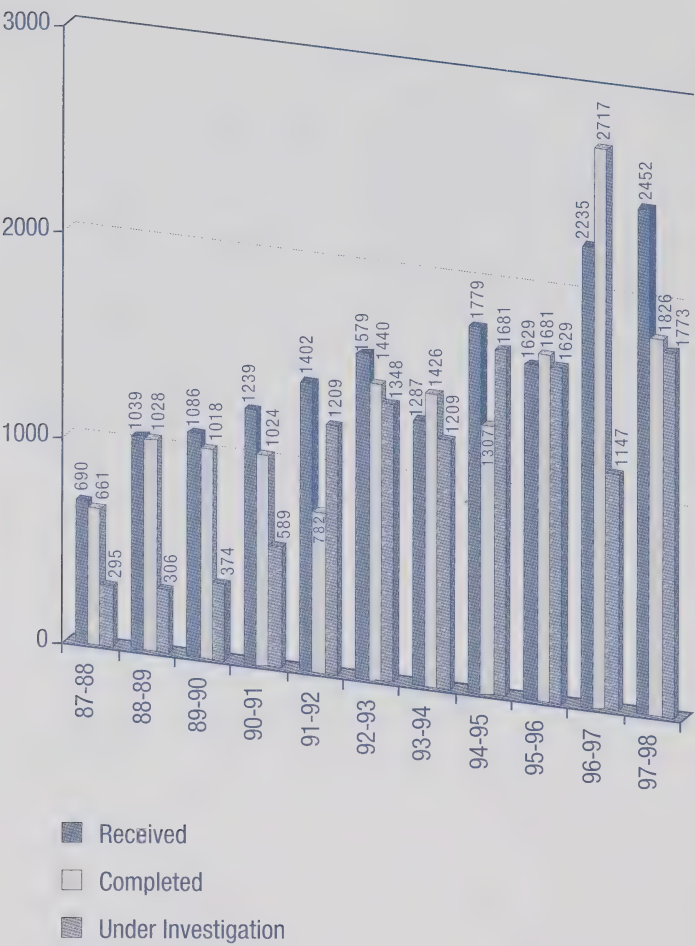
Investigations Completed by Grounds



Completed Investigations and Grounds 1987-98



Complaints 1987-98



* The chart reflects minor adjustments to 1993-94 to 1995-96 count

Origin of Completed Investigations

Newfoundland	14
Prince Edward Island	2
Nova Scotia	45
New Brunswick	42
Quebec	393
National Capital Region Quebec	11
National Capital Region Ontario	276
Ontario	504
Manitoba	25
Saskatchewan	88
Alberta	151
British Columbia	253
Northwest Territories	2
Outside Canada	20
TOTAL	1826

A better window on privacy issues

The Privacy Commissioner's main function is to investigate complaints stemming from alleged breaches to the *Privacy Act*. But the Commissioner does more: two other components of his mission are to be an effective privacy guardian on Parliament's behalf, and to be Parliament's and Canadians' window on privacy issues.

These two roles demand that the Privacy Commissioner be able to give a professional assessment of the quality of the federal government's adherence to the *Privacy Act*, and his research and communications activities provide legislators and the general public with the facts necessary to make informed privacy judgments. These two responsibilities have now been merged in a single branch called Issues Management and Assessment/Fair Information Practices.

In 1994, following a major overhaul of all government institutions, the Office's former Compliance Branch changed the way it did business. Its small staff could no longer afford to conduct traditional reactive audit and follow-up activities. A new branch was created to focus on monitoring new legislation and programs and providing active advice and guidance to federal agencies. These agencies were grouped into four main envelopes, each assigned to a portfolio leader.

The past four years, however, have demanded further changes to enable the Commissioner to accomplish this part of his mission. Experience has taught portfolio leaders that not all agencies in their portfolios require equal attention. And major issues have recently surfaced in the federal government that require considerable involvement from portfolio leaders, often working as a team with one agency.

A good example is the still-ongoing restructuring of all of Human Resources Development Canada activities. As manager and delivery agent of many social programs, the department has the most extensive personal information holdings in all of the federal government. It also relies heavily on application of state-of-the-art information technology. Reviewing its performance required a coordinated effort of all portfolio leaders, with input from policy and research staff. While the notion

of portfolios remains useful, it can no longer be absolute; portfolio leaders will increasingly work on critical issues, whether confined to one agency or spread across government.

As well, the Office relies on a handful of policy analysts and research staff to perform four other key activities: monitoring issues and developments in Canada and abroad, researching specific topics of interest or urgency, developing positions and policies on new legislation, programs and issues. The branch is also a critical component of the Commissioner's public communications efforts, offering presentations and speeches to federal agencies and businesses, doing media interviews, replying to inquiries, monitoring new legislation and preparing submissions to Parliamentary Committees and government agencies, and participating in joint projects involving public or private sector agencies. These activities may well have had the most public impact in the Office's 16 years of existence.

But with the pace of societal and technological change accelerating in Canada and abroad, the Office must now step up and refocus its research and policy work. Our answer has been to merge portfolio and research/policy staff to help feed and support one another. Essentially all of this report's material not dealing with specific complaints or legal matters are the product of this unit.

Electronic Commerce — A marketer's dream... a privacy nightmare?

The advent of “electronic commerce” virtually transforms the way we shop and do business. Electronic, or e-commerce, generally means the commercial transactions that take place between individuals and organizations over computer networks.

Certainly, this new kind of commerce offers huge potential for businesses to reach new customers, and for customers to reach businesses. Although much of current e-commerce focusses on buying services — such as banking on-line — rather than products, governments and businesses around the world are actively engaged in establishing a framework for purchasing goods electronically.

To help prepare Canada for the electronic marketplace, the federal government recently released two discussion papers; one dealing with protecting personal information in the private sector, and the other with encryption of electronic communications. Despite the initiatives, a lot of work remains to be done to protect the privacy of Canadians. Please see pages 11 and 60 for more detail on, and the Commissioner's response to, these initiatives.

These discussion papers, and the initiatives they propose, are on a tight schedule. They form part of the federal government's preparation for the Organization for Economic Co-operation and Development (OECD) and Government of Canada Ministerial-level conference on electronic commerce to be held in Ottawa in October 1998.

Thankfully, protecting privacy is on the conference agenda. Work is also underway to tailor the OECD's 1980 Privacy Guidelines to today's global networks. The OECD proposes presenting these guidelines to the Ottawa Conference in October for endorsement.

OECD member countries seeking to build effective privacy protection should consider a more recent and forceful initiative than the old OECD guidelines that were developed before electronic commerce was ever contemplated. An excellent foundation could be the EU Directive on protecting personal information which, beginning in October 1998, will protect the privacy of over 350 million European citizens in both the public and private sectors.

The federal government wants to be seen to be a world leader in electronic commerce, and understands that Canadians' trust in networks is fundamental to their participation. However, central to the interaction between information technology and the personal information it processes is the degree to which we respect each other as individuals. We know that technological change is making a shambles of the right to privacy. The measures the federal government has taken to date will be insufficient to protect privacy given the dangers that are inherent in electronic commerce.

Consider one of the newest methods of collecting personal information — capturing data sent over the Internet. Any move we make and information we submit online feeds valuable information to a huge market for personal information. Without your knowledge, and certainly without seeking your consent, a record is kept of every screen on every Web site you visit. Collecting this so-called “clickstream” data allows others to gather information on all the services or products that you buy online. But this information could also be matched with your Web surfing habits to develop a very personal profile of your preferences and dislikes — a marketer's dream.

A consensus seems to have formed that people should be forced to identify themselves when they want to buy something on a network. However, many of the face to face transactions that we now conduct are anonymous — a cash purchase, for example. Insisting that we reveal our identity to engage in electronic commerce would end a long history of anonymity and create new and more detailed trails of personal data that would chart our every move.

The development of new services (see *Internet — still no privacy*, page 65) may well enhance users' privacy. However, it is difficult to evaluate their merit because thinking about privacy in electronic communications is still in its infancy. One thing is certain; Canadians must become better informed about how technologies can lead to the misuse of their personal information. Once we understand that organizations can choose to use technology responsibly or irresponsibly, then we can hold organizations' management — rather than the technology — accountable.

Can we keep a secret?

In this age of computers, personal communications devices and global networks like the Internet, we rely heavily on a technology that is not secure. Anyone can access our data and our communications unless we take special steps.

Fortunately, the technology also exists to prevent unauthorized access. Encryption transforms our voice communications, electronic mail, computer documents or fax communications into code during transmission and storage. Even if others gain access to the message, they cannot understand it without the proper code. Encryption provides an added benefit; it also allows us to confirm the identity of the sender, and that the communication has not been altered in transit.

An encryption primer There are two main cryptographic methods. The first, “private key”, uses the same code (or “key”) both to transform information into meaningless strings of characters, and to undo the transformation. Both sender and receiver must protect their key.

The second method, “public key”, uses two keys working together: a public key which the sender uses to transform the information before sending it, and a secret key, known only to the recipient, which is used to decode the message. The secret key can unlock only the information transformed by its corresponding public key. This method is increasingly popular because it is much easier to use on a large scale. Publishing a public key is a one-time step, rather like publishing one’s telephone number. Disclosing our private key to every person with whom we might want to communicate could become onerous and, once disclosed, the key could be beyond our control.

The effectiveness of a cryptographic product relies on the length of the keys it uses, measured in “bits” (one letter or digit in a word or number is a bit). Cryptographic keys are mathematical formulas which can range from eight to over 2000 bits in length (most are between 40 and 128 bits). The higher the number of bits, the more secure the key because the longer it would take to decode. To illustrate, it would take less than four hours to decipher a 56-bit key using today’s technology, but multi-million years to decode a 112-bit key!

On the other hand... So cryptography may have solved the electronic security problems. But there, according to law enforcement officials, is the rub; if you can protect your communications by encrypting them, so can criminals. And if they cannot access and understand coded information, police argue, they cannot enforce the law effectively. Thus law enforcement officials want us to use cryptography only if they can have the keys to unlock the coded information. This proposal is not unique to Canada: police forces from many Western industrialized countries seek similar conditions, and have agreed (in the “Wassenaar Arrangement”) to control the use of cryptography.

In this instance, however, law enforcement interests run directly counter to the individual’s privacy and to business interests. Few will want to use the Internet to send sensitive information such as a medical record, a credit card number or proprietary secrets if this information is not protected. The proposal is somewhat akin to requiring everyone to give local police the keys to our homes in case we might commit a crime in the future and they need to enter.

The scope of this proposed access is unparalleled and moves us a step towards a police state. The proposal could also be counterproductive. Public knowledge that our electronic communications would be either unprotected or open to law enforcement interception could weaken public confidence and thus reduce the power and appeal of such projects as electronic commerce.

With an evident need for a policy, and the debate raging, the federal government issued a discussion paper in February to consult Canadians. The government focused on the use of cryptography for electronic commerce, and sought comments in three policy areas: access to stored information, access to communications, and restrictions on the export of cryptography products using keys longer than 40 or 56 bits.

The Privacy Commissioner’s submission observed that “the broad interception and decryption capabilities sought by law enforcement agencies may not be the most appropriate solution to the problem of criminal activities, and may violate Canada’s *Charter of Rights and Freedoms*. Indeed, law enforcement agencies have not proven that the interception and decryption capabilities they are seeking will lead to a

decrease in criminal activities.” The onus is on government to demonstrate an overwhelming public interest before overriding our right to have private communications.

The Commissioner also recommended that

- All Canadians should have access to cryptography;
- Canadians should be able to choose freely whichever cryptography product, if any, they want to use;
- Canadians should be able to decide freely on how to handle their cryptographic keys;
- Cryptographic keys and coded information should be stored securely; and
- All electronic commerce activities should allow cryptography.

Industry Canada is now reviewing responses to its discussion paper.

Stick Before Carrot

Treasury Board Secretariat Policy on the Use of Electronic Networks

The federal government increasingly relies on electronic networks — the Internet and electronic mail systems, among them — to conduct its operations. Understandably, government is concerned that employees use these networks only for government business and not for unlawful or unacceptable purposes.

In February 1998, Treasury Board Secretariat published its “Policy on the Use of Electronic Networks”. Among the requirements the policy imposes is a duty for each organization’s senior official to develop statements for employees indicating that unlawful activity is not permitted on these networks, and that certain other activities may be lawful but, nonetheless, unacceptable. We applaud the policy on this point, since these statements will help clarify the expectations of employers and the rights of employees.

The policy allows an organization to refer suspected misuse of networks to an appropriate official for investigation under two conditions: if it receives a complaint; or if its routine analysis of electronic networks (which does not involve reading the content of electronic files or mail) leads it to suspect that a person is misusing the network. Investigation may involve special monitoring or reading of the contents of electronic mail and files.

The policy also deals with government employees’ expectation of privacy. It notes the *Charter of Rights* guarantees that give government employees a right to a reasonable expectation of privacy, even if the employees are using government computers. However, the policy seems to suggest that an employer can diminish that reasonable expectation of privacy by telling employees that monitoring will occur.

This position seems to imply that simply telling employees that their electronic activities will be put under increased surveillance reduces the *right* to a reasonable expectation of privacy. If that were the case, then other types of highly intrusive employer surveillance — such as putting cameras in washrooms — might also be permitted simply by telling employees it would happen. Such an interpretation (we hope unin-

tended by the Secretariat) could lead to the serious and arbitrary erosion of the privacy of government employees.

We are not saying that surveillance of employees is never justified. However, we are deeply concerned about a policy that might see federal employers assuming a broad right to monitor the electronic activities of employees without specific justification.

At a meeting with Treasury Board staff to discuss an earlier draft of the policy, we raised several points, including the following:

- A government policy that allows extensive intrusions will almost certainly be held up by the private sector as justification for similar intrusive policies. Therefore, the government policy should go no further than is absolutely necessary to achieve the government's legitimate goals as employer;
- It is preferable, whenever some intrusion is warranted, to use the least intrusive option first. This means starting with education setting out clearly the acceptable and unacceptable uses of electronic networks. Only if that does not resolve the problem should intrusive solutions such as monitoring be considered acceptable.

Treasury Board Secretariat did make some adjustments based on our recommendations. However, the final policy still contains excessive powers of intrusion. In particular, the Secretariat appears to have rejected our call to use the least intrusive measure first, moving to greater intrusion only if the less intrusive measures proves ineffective. The policy clearly contemplates monitoring the contents of e-mail and the Internet web sites visited, yet does not provide sufficient limits on when such intrusive measures can be used.

In addition, the Secretariat appears to consider e-mail inherently less private than a telephone conversation, since the policy envisages monitoring e-mail without the consent of the sender or recipient. Monitoring of a telephone in this manner would be a criminal offence.

Federal employees may not all be angels. Some, like their private sector counterparts, may not be entirely productive or honest in their dealings. However, that does not justify making all federal employees, most of whom can be trusted to act perfectly responsibly, the target of heavy handed monitoring.

Internet — still no privacy

The 1995-96 Annual Report gave readers some tips on how to protect their privacy on electronic networks (*Privacy in Cyberspace: a Surfer's Guide*). Two years later, the Internet has become much more commercial (to the point that some governments are looking at ways to tax on-line purchases!), and privacy is at even greater risk. There are currently four main types of privacy invasions on the Internet:

On the World Wide Web

The biggest Internet privacy invasion is the collection of your personal information without your knowledge — information that can be used, rented or sold to on-line and other direct marketers. And this applies to both information about yourself and about your activities on the Web...

- Your electronic mail (“e-mail”) address, sometimes your name, your Internet Protocol (“IP”) address (from which your rough geographical location can be inferred using a domain name lookup service), the type of browsing software you use (and by implication, the operating system of your computer). Fortunately, most of this information can be withheld from Web sites if you first surf through such sites as the Anonymizer, at [www.anonymizer.com].
- Information about your activities on the Web (also known as “clickstream information”): who you are, when you enter a site, the last page you accessed (required for the BACK function of your browser), which sections of a site you go to and how much time you spend on each, what documents (or pictures) you download onto your own computer, and what information you search for with such well-known tools as AltaVista or Yahoo. As above, your clickstream information can be also be anonymized by first going through certain sites.

Web sites may also store some of this information on your own computer in the form of a “cookie” file. This allows the site to retrieve the information at your next visit, and “personalize” its greetings. However, you can instruct your computer to refuse such cookie files.

As well, some municipalities and government institutions are increasingly interested in using the World Wide Web to post information for the general public. While the intended convenience is usually laudable, the end result can be disastrous. The cities of Victoria, B.C. and Aylmer, Québec (among others) had to remove sensitive financial information from the Web following the public outcry that ensued. While tax rolls are usually publicly available information, it is a quantum leap from a personal consultation of tax records at a local city hall to providing over 40 million computer users worldwide a person's address, property value, taxes owing and (in some jurisdictions) religious affiliation — all from the comfort of their homes. Similarly, Manitoba Telephone Systems had to remove billing information from the Web following protests by its subscribers.

On the Usenet

Participating in discussion groups on the Usenet can lead to a second, less well known privacy invasion. Every message you post to a discussion group is archived for others to search. Not only are your personal views on a given topic stored permanently, it is also possible to search the Usenet to find out which discussion groups you participate in, and thus determine your interests (DejaNews — the message archivist — does allow you to delete selected messages). Even worse, it is also possible to find out who is looking at a message at a given moment!

Writing e-mail

You will never hear it enough: e-mail on the Internet is as private and secure as a post card in the “snail mail”. Everyone from your Internet provider staff to your correspondent's friends or colleagues can read your electronic message from the moment you click “SEND” on your computer. Unless you and your correspondent use encryption (see *Can we keep a secret?* page 60), avoid including sensitive information such as credit card numbers, vacation dates or medical information in your electronic messages. You could also use anonymous remailers which forward your message, and sometimes the reply, without including any personal information. Among others, you can find a good list of those remailers at our Web site.

Another privacy invasion prompted by e-mail is junk electronic messages, better known as “spam”. Once an on-line direct marketer gets hold of your e-mail address, you will find unsolicited electronic advertising in your mail box. Because junk e-mail is as much a nuisance as regular junk mail, and because it is costly to you (keeping you connected while you receive, read and delete the junk messages), most Internet Service Providers (ISPs) have devised ways to block spam from your e-mail box. Inquire!

Hacking

Hacking is the unauthorized access to computer systems and files. And the best electronic protections (such as “gateways” and “firewalls”) can, and do, fail. Because the Internet is nothing more (and nothing less) than a worldwide electronic computer network, it is a hacker’s paradise. Getting access to your ISP’s file listing of all of its users’ names and passwords would be a dream for a hacker who could then read, redirect, change or delete your e-mail without your knowledge. Some hackers prefer shopping and try to hack ISP or Web site files containing credit card numbers. Others are more interested in company or personal secrets and will look for interesting business or personal information they could resell or misuse.

This is not just the stuff of movies: last year alone the best protected computers in the world; those of the Pentagon, the FBI and NASA were successfully hacked hundreds of times! And if you think your information is of little interest, think again: some hackers specialize in stealing enough information about you to impersonate you; ordering credit cards in your name, renting or buying in your name, holding a job in your name — leaving all the bills and income tax to pay (not to mention a reputation to rebuild) also all in your name! This is the growing problem of “identity theft” which is exacerbated by electronic transactions.

Are there solutions to all of these privacy invasions?

Aside from these tips, there is little to protect your privacy on the Internet. Laws would be of little use because laws change from one country to the next, and the Internet knows no borders. Codes of

ethics (like the December 1996 Code of the Canadian Association of Internet Providers) are nice statements of intent but they are voluntary and useless if they are breached. Yet, two new solutions have recently appeared which could make a difference — if they work.

The first is TRUSTe. Launched by a group of American companies and advocacy groups in June 1997, the program encourages Web sites to tell surfers about their privacy protection practices and what they do with the personal information they collect. Sites that subscribe to TRUSTe display the program logo or “trustmark” on their welcome page (and can be audited at random for compliance). Unfortunately, few sites have joined the program — by April 1998 it had attracted only 75 participants. Apparently one major factor in companies’ hesitation is TRUSTe’s sanctions for those which do not comply with the guidelines. However, businesses that are serious about gaining clients’ trust by protecting their privacy in an electronic environment should embrace this attempt at self-regulation, rather than waiting for legislation to force them to comply.

The second solution is the Platform for Privacy Preferences Project (or “P3P” for short). Begun in May 1997 by the consortium that oversees the development of the Web, the project allows surfers to specify their privacy protection preferences (through their browser), and Web sites their privacy protection practices. Surfers can then access compatible sites, and choose to either stay away from, or negotiate with, incompatible sites. P3P is still under development, however, and will not become fully operational for several months. Its future is uncertain, as is its popularity with Web site owners.

When it comes to the Internet, the sad truth is that there still more money to be made by invading your privacy than by protecting it. Until that changes, beware!

But a useful tool

Privacy Forum — an Experiment in Electronic Democracy

For those who missed it, the government's discussion paper on private sector legislation (see page 11) was made public January 24, and the window for comments closed on March 27! That left little time to get busy people from across the country involved in debating how the private sector should protect their personal information.

But a coalition of public interest and consumer advocates from across Canada managed it. They mobilized at lightning speed to respond to the paper's call for comments by building an interactive web site and discussion group called the Privacy Forum.

The project was spearheaded by the Media Awareness Network, the Public Interest Advocacy Centre, Canada's Coalition for Public Information, the Consumers' Association of Canada, the Fédération nationale des associations de consommateurs du Québec, the Ottawa Public Library, and Telecommunities Canada. This Office provided administrative support.

The Web site contained background information on privacy issues and links to other relevant sites, as well as an online survey for Canadians to express their views on privacy protection. The Forum also hosted a discussion group to allow people to talk to one another about privacy issues.

The purpose of the Forum's survey was not to gather scientific polling data but rather to determine people's responses to strongly worded statements about information privacy protection. The survey results revealed a strong consensus on several issues.

One of the clearest messages — and one this Office heartily supports — is that respondents are dissatisfied with current information practices in the private sector. They expressed particular annoyance with telephone solicitations, junk mail, data trails and the general exchange and sale of personal information.

While respondents were quick to acknowledge that the government has privacy laws, many expressed concern about how governments collect and use personal information. Survey respondents also voiced strong support for keeping control over their personal information and not being penalized by companies for refusing to provide it.

In addition, respondents felt that the complaint process should be simple and it should have safeguards to ensure that companies are in compliance. Finally, virtually all respondents saw a need for education about privacy issues.

Overall, the Privacy Forum web site was a great tool both to inform Canadians about privacy issues and to assess their responses. Hosted through a part of the Media Awareness Network's web site called the Privacy Pages, the Privacy Forum had links and background material to spare. And inform it did. More than half of the 266 survey respondents said the Privacy Forum had both increased their understanding of and — perhaps more importantly — changed their minds about, privacy issues. Now that's results. Who knows how many more people would have participated had there been more time; another 100 people completed the survey after the deadline had passed.

This experiment in electronic democracy was a resounding success, all the more considering the tight deadline. The coalition's extraordinary effort to engage Canadians in the debate was one of the highlights of the whole exercise.

A Privacy Playground for kids

Making kids more informed Cybersurfers has been a priority of the Media Awareness Network since its launch in 1996. Now the Network has found a way to teach young children to protect their privacy on the Internet.

In mid-May the Network released its Privacy Playground: the First Adventure of the Three Little CyberPigs game on CD-ROM. The game features the three little cyber-pigs and a big, bad cyber-wolf in interactive situations to teach children how to recognize invasive and deceptive online advertising, and the importance of not divulging personal information online.

The Media Awareness privacy web site is also worth a visit for the largest Canadian collection of online educational materials on privacy.

Looking forward to Private Eyes

High school students have not been forgotten. Beginning this Fall they can participate in the Private Eyes Project which celebrates the 50th anniversary of the signing of the United Nations Universal Declaration of Human Rights. The Declaration recognizes the importance that privacy plays in protecting human rights.

The project is the brainchild of the Human Rights Research and Education Centre at the University of Ottawa with generous support from the Royal Bank of Canada, Canadian Heritage department, Sheila Finestone, MP, former chairperson of the Standing Committee on Human Rights and the Status of Persons with Disabilities, as well as this Office. The Law Room site is part of Canada's SchoolNet. It provides site visitors with several scenarios which challenge us to weigh the evidence and draw our own conclusions about the value of protecting our personal information. An added bonus is the project's practical information about the process of Parliamentary committee hearings and intergovernmental negotiation.

Students will be make practical use of the information this Fall when schools across Canada participate in the interactive unit of the project. Schools are invited to conduct their own mock parliamentary hearings on privacy rights in the next century and then publish their findings in the Law Room. The next step will be to discuss the issues in a national online forum, then selected schools will negotiate an intergovernmental agreement on privacy rights over the Internet. The agreement will then be submitted to participating schools for ratification.

The entire Law Room site delivers high-quality educational materials on justice and human rights issues to teachers and students. Although designed for high school students, the site merits a visit from everyone who has questioned how technology is changing our lives, and how to balance technological progress and human values such as privacy.

Links to both these sites are available through the Office's Web site.

The Privacy Pages — Industry Canada's Online Commitment to Privacy

Industry Canada's Task Force on Electronic Commerce has also developed a web site which both explains the need for privacy when conducting electronic transactions, and provides a "Privacy Toolkit" to help people protect their personal information.

The toolkit provides information on Consumer Education, Codes of Practice, Legislation and Privacy-Enhancing Technologies and, of course, a link to the Discussion Paper on private sector legislation entitled *The Protection of Personal Information: Building Canada's Information Economy and Society*.

You can link to Industry Canada's Privacy Pages on our Web site.

The DNA Databank Bill — Still

Last year's annual report discussed at some length the DNA legislation that had just then been introduced in the House of Commons. The proposed *DNA Identification Act* sought to establish a DNA databank of samples taken from convicted offenders to help police identify those responsible for unsolved crimes. The bill was the second phase of the government's plan to regulate DNA testing as a tool to identify unknown offenders who leave traces of DNA at the crime scene. The first phase of the law allowed police to obtain a warrant to obtain DNA samples from *suspects* and was enacted in 1995.

With the April 1997 general election, the databank bill died on the order paper. In September 1997 the government introduced almost identical legislation, Bill C-3, several aspects of which give cause for concern. In his March 1998, appearance before the Standing Committee on Justice and Human Rights, the Commissioner made several recommendations, among them:

- taking DNA samples only from those convicted of a violent offence for which there is a high risk of re-offending and a likelihood that genetic material would be left at the crime scene;
- destroying the DNA samples after extracting the identification information, leaving only the analysis on police files, and
- ensuring that DNA samples and analysis volunteered by individuals to help police exclude them as possible suspects, be destroyed immediately after use and not be used for a “fishing expedition” to determine responsibility for any other crime.

We remain troubled by pressure from some groups and politicians to impose automatic forensic DNA testing on anyone charged with an indictable offence, which could include acts as relatively minor and non-violent as swearing a false affidavit. DNA would then be taken from most criminal suspects (since most *Criminal Code* offences are indictable) almost automatically, as are traditional fingerprints.

The Department of Justice strongly opposed this attempt to expand the scope of DNA testing of suspects on constitutional grounds. We oppose expanded testing because it constitutes an excessive and unnecessary use of intrusive state powers that should be exercised only in tightly controlled situations, and only after a judge's warrant authorizes the intrusion.

As this report goes to press, the bill had been withdrawn.

Position papers on both issues, compulsory collection of DNA samples from suspects in a specific crime, and establishment of a DNA database, are available from our office and at our Internet web site.

The Year on the Hill

Canada Labour Code Bill C-19

This legislation governs labour relations in federally regulated industries such as banking, telecommunications and transportation. The Commissioner expressed reservations about a number of amendments to the code contained in Bill 66 in the previous Parliament. With the calling of the 1997 election, the bill died on the order paper.

A slightly modified Bill (now C-19) was introduced in November 1997. In his appearance before the Parliamentary committee, the Commissioner highlighted two clauses which caused concern. The first, clause 50, states that unions will be able to communicate with off-site workers. Since this requires employers, and occasionally the Canada Labour Relations Board (CLRB), to provide the off-site workers' place of work, for many that meant disclosing their home addresses.

Pointing out that most individuals have a high expectation of privacy at home, the Commissioner asked that the bill require workers' active consent to disclose a home address, rather than an opt out. Union membership is not compulsory and unions could canvass off-site workers at the employer's business address. For example, the *Public Service Staff Relations Act* requires federal government agencies to provide new employees with a union registration card which they can complete and return as they wish. Public service unions do not receive home addresses from the employer.

The second clause (54) specifically prevents individuals from having access to their personal information contained in notes taken by appointees of the CLRB or the Minister without the appointees' consent. This appeared to provide the Board members, arbitrators or anyone assisting the Board with special relief from both the *Privacy Act* and the *Access to Information Act*. While boards and agencies may sometimes find it administratively inconvenient to operate under the openness provisions of both laws, they are "there to protect Canadians, not bureaucrats and appointees", the Commissioner told the commit-

tee. He urged the committee not to let individuals or institutions craft their own little set-asides and exemptions from laws such as the *Privacy Act*.

Of greater immediacy, perhaps, was that this very issue is before the Courts. A man complained to the Commissioner of being denied access to personal information in the notes of the CLRB member who heard his case. The Board argues that members' notes are not under CLRB control. The Commissioner considered the complaint well founded and appealed the Board's continuing refusal to the Court. He urged the Committee to await the Court's ruling before proceeding on this amendment.

As we go to press, the bill has received Royal Assent. The legislation now gives the Board the power to order employers to provide names and addresses of off-site workers to unions. The order must specify the method of communication, times of day and periods during which the communication is authorized and the conditions which must be met to safeguard the employees' privacy. If the Board considers that employees' privacy and safety cannot otherwise be protected, it may seek their consent for the disclosure. The weakness of this solution is that it acknowledges the privacy issue at stake, but resolves it by giving discretion to the Board to make the privacy determination for the employee.

Parliament also rejected the recommendation to await the court's decision on access to Board members' notes. Not only may these be accessed only with the member's consent, the exemption is extended to anyone appointed by the minister and the Board to help in resolving complaints or issues in dispute before the Board.

Canada Pension Plan Act

Among extensive amendments to the *Canada Pension Plan Act*, were several dealing with access to, and disclosure of, individuals' personal information in pension files. In an effort to loosen the stringent protection provided this information by existing Canada Pension and Old Age Security legislation (which Human Resource Development

Canada — HRDC — argued hampered its internal operations), it proposed substantially broader discretion for the Minister and greatly expanded permissible collection, uses and disclosures.

The bill also contained a sort of truncated — and flawed — *Privacy Act* which appeared to hedge individuals access rights and built in no notification to the Privacy Commissioner for public interest disclosures.

The greatest danger in this approach is that clauses dealing with disclosures of personal information in other acts of Parliament override the specific limitations in the *Privacy Act*. In short, in the interest of achieving greater flexibility in its own enabling legislation, the department risked gutting the *Privacy Act*. The Commissioner acknowledged that while that may not have been the intent, it was indeed the effect. He recommended HRDC require that any uses and disclosures be “consistent with” the original purpose for collection rather the blanket permission allowing the Minister to disclose “for the administration of another federal law, a provincial law or an activity”. The Commissioner suggested the department consider the approach taken in the *Income Tax Act* which sets out the limited and specific disclosures allowed.

The bill allowed similarly broad collection from federal and provincial governments, their public bodies and non-government bodies without any attempt to limit the collection to information relevant to administering the CPP, or even to any HRDC program.

Following several meetings, and on the eve of the Commissioner’s scheduled appearance before the Standing Committee on Finance, HRDC and Office staff negotiated several amendments. These included making it clear in law that individuals retain all existing *Privacy Act* rights, limiting sharing with federal institutions to those required to administer the CPP Act, removing references to provincial “activities” as legitimate for disclosures, and including specific references to non-HRDC programs which require CPP data to administer programs. Similar changes were made to the *Old Age Security Act* proposals.

As in any negotiation, no-one got everything they wanted, but all got something they could live with. We commend HRDC staff for their sensitivity to their clients’ privacy and their determination to do the drafting properly.

Task Force on the Future of Financial Institutions

The Task Force was created to examine the structure and policy issues surrounding the financial institutions and non-traditional providers of financial services. It is expected to report in September 1998.

The Commissioner made his first submission to Parliament about protecting the privacy of customer records in 1992 when new legislation changed the whole regulatory scheme for financial institutions. The report discussed the privacy threats posed by newly permitted cross-ownership of financial services. These include sharing customers' personal information among affiliated institutions, as well as the technological capacity these institutions have to collect and assimilate the personal data and profile their customers.

In this report and subsequent submissions to Parliamentary Committees, the Commissioner recommended the government act on its power to make regulations to protect customer records. In the meantime, financial institutions have entered yet another line of business — processing other companies' data.

The upshot of several committee hearings and reports was to write regulations requiring financial institutions to establish procedures governing the collection, retention, use and disclosure of customer information, to inform customers of these procedures, to appoint an internal officer to deal with complaints, and report annually on the complaints — all steps the industry had already taken. The Canadian Bankers Association has implemented the Canadian Standards Association Model Code and appointed an industry ombudsman.

While this appears to be progress, two essential ingredients are missing: actionable rights and independent oversight. Nothing requires a financial institution to open its doors to independent arbitration or audit. Without these components there is merely a mirage of privacy protection. Six years labour seemed to have brought forth a mouse.

Hope for effective privacy protection in financial institutions now rests on an effective law for the federally-regulated private sector, promised for the year 2000 (see page 11).

Updates

Private Phone Directories: the End of the Saga

As previous annual reports have demonstrated, subscribers' personal information as published in telephone company directories, is worth its weight in gold. But, happily, subscribers have won back some control over this information.

Four years ago, independent directory publisher White Directories of Canada asked telephone companies for their customer databases in order to publish its own directories. The Canadian Radio-Television and Telecommunications Commission (CRTC) agreed on condition that subscribers' consent be sought. White Directories appealed the CRTC decision to the Governor-in-Council arguing that this could make White's directories less complete. The Governor-in-Council agreed with White but ordered the CRTC to examine the broad privacy protection of subscribers' personal information.

In December 1996, the CRTC reported back to the Governor in Council, acknowledging the privacy problems and signalling its intent to hold public hearings on the whole issue of opting out of directory listings. Among the Commissioner's recommendations to last Fall's hearings was one suggesting that the CRTC examine the cost of being unlisted which — at more than five dollars monthly in some provinces — was a deterrent to some who might otherwise choose to opt out.

In its Order 98-109 (February 1998), the CRTC set a maximum monthly charge of two dollars for unlisted service and ordered telephone companies to allow subscribers to pay in installments any charges for changing their numbers. The CRTC rejected the Commissioner's other recommendations that unlisted service be free and, for the fourth time, that unlisted subscribers have automatic line blocking to prevent their number's display. This refusal means that unlisted subscribers must remember to dial *67 (or 1167 for rotary dials) every time they call.

Although less than we hoped, this latest order may help reenforce subscribers' privacy by bringing unlisted charges within reach of more who may be interested. But don't let down your guard yet. Everyone

should read carefully the introductory pages of the local telephone directory which explains the company's special services and how they affect privacy. Too few people take the time to learn about how to remove their names from paper directories, call display, electronic directories on Internet (such as Canada411) and lists sold to marketing companies.

Ten minutes spent reading may help prevent some of those annoying carpet cleaning solicitations at dinnertime, or stem the tide of junk mail in our mailboxes.

Permanent Electors Register

Elections Canada continues to keep the Office abreast of its administration of the permanent voters' list. The list, created for the last federal election from a final enumeration, can be updated from citizenship and income tax databases with individual's consent, and from various provincial sources.

The *Elections Act* also allows Elections Canada to enter agreements to share lists of local voters with provinces and municipalities to help them draw up lists for local elections — providing individual voters consent. These lists (minus names of those who did not consent) have already been given to several provinces and municipalities which have signed agreements with Elections Canada.

Shortly after lists were given to the New Brunswick and Winnipeg governments, several voters wrote to Elections Canada to opt out. Since it was too late to remove the names from the federal list, Elections Canada asked both governments to remove the names from local lists if the federal list was their only source.

Given that this was in itself a disclosure of personal information, but one that is consistent with individuals' exercising consent, Elections Canada also advised that it would amend its description of the bank in *Info Source* to make clear the possible disclosures.

Elections Canada has assured the Commissioner that all future agreements will include clauses requiring other levels of government to comply with these requests (existing agreements will also be amended).

On another note, the project to seek taxpayers' consent for updating the electoral list from their income tax files appears to have succeeded. Despite some early nervousness, about 81 per cent of taxfilers agreed to the transfer — an indication that informed consent does work.

Incidents

The Canadian Wheat Board alerted the Commissioner in early March 1998 that an MP and the Canadian Farm Enterprises Network had given the media a list containing exact salaries of all Board staff and members. The list included all staff, management and Governor-in-Council appointees — some 400 people. While the *Privacy Act* allows some information about employees to be released — specifically exempting it from the definition of “personal information” in the interest of public accountability — exact salaries are protected.

Apparently the list was drawn up annually until 1996 to place new staff in the appropriate salary range according to their experience and qualifications, and the range of existing employees doing the same work. Senior management also used the list during annual performance reviews to ensure consistency across the organization. Access to the list was tightly controlled to two senior executives and their secretaries, the person who prepared the list and another who analysed it for reports to senior management, and the director general of personnel.

The Board confirmed that the list in the hands of an MP and the Canadian Farm Enterprises Network is a copy of the original. Given the intense political debate in Western Canada over Board staff salaries and its mandate, the disclosure was likely the classic plain brown envelope leak.

The Board has hired a private company to investigate and will keep the Office informed as investigation progresses. It will also provide a copy of the investigation report. The Commissioner agreed to await the outcome of that investigation but reserves the right to make his own inquiries.

“Sharing agreements” become visible

Virtually all privacy legislation contains clauses allowing governments to share information to administer or “enforce” various benefit programs. While some sharing is understandable, its extent is mushrooming. Much of it is virtually invisible to a public not regular readers of the *Canada Gazette* or other arcane government publications. And *Info Source*, the federal government’s directory of personal information holdings, describes sharing in very general terms.

Sharing is not confined to the federal government, of course. In fact, data is often shared among federal, provincial, municipal — and sometimes even international — governments. The *Privacy Act* allows sharing “under an agreement or arrangement” to administer or enforce any law or carry out a lawful investigation. These agreements do not require the individuals’ consent and, although they oblige the government to advise the public, notice usually appears only in *Info Source*.

Clear notification can have interesting consequences. A recent example is a provincial sharing agreement which, once spelled out for the public, unleashed a firestorm of criticism in British Columbia. When new legislation came into force in April 1997, the BC Ministries of Human Resources (MHR) and Education Skills and Training (MEST) wrote to those receiving Income Assistance, Youth Works and Disability benefits. The letter advised that recipients were “required to consent” to the ministries collecting information about them from various other organizations. The operative paragraph reads:

“I give my permission to any person having such relevant information or documents to release them upon written or verbal request to employees of MHR or MEST. I understand examples include, but are not restricted to, information or documents from: Human Resources Development Canada, Workers Compensation Board, Insurance Corporation of British Columbia, British Columbia Student Assistance Program, Motor Vehicle Branch, British Columbia Assessment Authority, Registrar of Companies, Land Titles, Lottery Corporation of British Columbia, Vital Statistics, Old Age Security, Canada Pension Plan,

federal, provincial or municipal government departments, and the Department of Citizenship and Immigration Canada, police, federal or state related aid agencies from the United States of America or any other country, Equifax, any bank, credit union, cheque cashing service or other financial institution, any landlord, and past, present or future employers of myself or my family members.”

A separate box authorized Revenue Canada to disclose “income tax returns and other taxpayer information”.

Astonishing as the list is, it may well be the first forthright description by any government of the scope of its information collection to police social programs. Collection on this scale would not have been possible without the advent of powerful information systems which match data from one system to another, usually by exchanging computer tapes.

Shortly after the letters went out, the Office’s telephones began ringing. Given the scope and the lack of specifics on what was to be collected from the federal departments — Human Resources Development Canada (HRDC) and Citizenship and Immigration (C&I), Office staff asked for details.

HRDC reviewed the form and alerted its BC Region staff that “The form is not acceptable for the disclosure of information held by HRDC as it fails to provide sufficient facts to allow individuals to make an informed decision to consent or to refuse”. The department will continue releasing specific information under a long-standing agreement with the MHR. Information is shared to ensure that applicants are not drawing both employment insurance and welfare, or that their benefits are adjusted accordingly.

All the information is drawn from the (Un)employment Insurance Claim File, Record of Employment File and/or Benefit and Overpayment Master File. It includes name and last known address, Social Insurance Number, case identification and various details on when benefits were begun, the weekly rate, claim status and type, waiting period and previous occupation. HRDC may also provide other details “for investigative purposes” on “written request”; however, these

disclosures require Headquarters' authorization. Any disclosures to MEST require the individual's consent.

Citizenship and Immigration Public Rights staff faxed an advisory to its BC staff, reminding them to release personal data to MHR only in accordance with the 1997 Memorandum of Understanding. The memorandum sets out clearly what information may be released, how and when, and overrides any individual's signed consent form. The Office is investigating several formal complaints against Revenue Canada.

Apparently the proposed collection was discussed with BC Information and Privacy Commissioner David Flaherty who reviewed the legislation and sharing agreements. Despite his concern, he had to conclude that the ministry had the "legislative authority to contact any agency that it considers necessary in order to verify eligibility for benefits". Dr. Flaherty was instrumental in having the application and consent forms spell out the details, thus making it "transparent".

In a public statement (issued January 27, 1998), he observed "That data collection is sanctioned by law does not in any way lessen its negative privacy impact on those receiving benefits. However my power is effectively limited by the fact that the Legislature can invade personal privacy by law or regulation, if this is determined to be in the public interest".

Several anti-poverty groups launched a legal action against the collection. In the face of the controversy, the MHR has revised the consent form, which is now an integral part of the application form, issued a fact sheet and a series of questions and answers on the benefits process for applicants.

Data Matching

The sparse data matching activity in the past year has been limited to Human Resources Development Canada (HRDC). While other institutions sent out feelers, often in the form of general questions on the process, once the whole approval procedure is explained — detailed assessments, cost benefit analysis and submission to the Privacy Commissioner — departments realize that this is no trivial matter. Sometimes the enquiries indicate more a need to understand data-matching rather than an intent to undertake one.

Canada Student Loan defaulters and the government employee database

This match, first described in last year's annual report, proposed running the list of those in default of their Canada Student Loans against the federal employee payroll. This would allow HRDC to identify those employees who have defaulted on loan repayment agreements and to recover any funds owed by an essentially captive audience.

The *Privacy Act* clearly permits disclosures of personal data to locate someone who has been established as owing a debt to the Crown or to whom the Crown owes money. This is distinct from matching lists in order to determine who *might* owe a debt, as in the match of Customs traveller declarations and employment insurance claimants. This is an important distinction.

Once the student loan program generated a list of defaulters and matched it with the government payroll, the Office's lingering concern was to ensure that recovering any debt not have negative impact on the employee at work. Unless it becomes necessary to garnish the employee's wages, the employer need not know that an employee has defaulted — it is a matter between employees and the Student Loan Program.

HRDC explained that it would contact only one officer in the employing institution — the official in charge of the payroll. Collection officers would try to obtain the employee's home address and telephone number and then deal with the employee at home. If a

satisfactory repayment plan can be worked out, the employer is not involved any further. Should garnishment prove necessary, arrangements will be made with the pay office, not the employee's supervisors.

Alberta Disability Income Program and CPP Disability benefits

This match compares the list of beneficiaries of the Canada Pension Plan (CPP) disability plan with those receiving payments from the Alberta Disability Income Program. Although currently limited to Alberta, HRDC is planning similar arrangements with the other provinces and territories.

The initiative, on the back burner for the past two years, is partly a response to a comment in the 1996 *Report of the Auditor General*. That report cited a 1995 Statistics Canada study showing that 17 per cent of those receiving CPP disability benefits were also receiving provincial Workers' Compensation Board benefits. The Auditor General estimated that CPP could save \$42 million annually by eliminating the duplicate payments. Curiously, this statement overlooks CPP's status as the first payer. Collateral benefits from the province do not usually affect entitlement to CPP disability benefits. This data match is more likely to produce savings for the Alberta program, not CPP.

Alberta provides HRDC a list of those receiving payments from its program (part of the Workers Compensation plan). HRDC matches the information with its CPP disability payments database, creates a list of those appearing on both databases and gives it to Alberta.

Although some individuals do legitimately receive benefits from both CPP disability and the Alberta program, many will find the Alberta payment reduced or eliminated. Only those suffering a prolonged disability will receive a CPP disability pension. In the interim, Alberta may pay the provincial disability benefit. Once CPP payments kick in, provincial benefits may be adjusted or terminated. Alberta may recover any overpayments and will almost certainly benefit by reducing program costs.

HRDC stated that matching two income replacement/support programs — CPP Income Security and the Alberta program — is a "consistent use" of the CPP disability information. The Office accepts

that using information about an individual receiving an income replacement pension to assess eligibility for, and amount of, collateral benefits can be considered a consistent use of the information.

To ensure a consistent approach at both ends, Office staff discussed the match with the Alberta Information and Privacy Commissioner's office. That office had reviewed the match with the provincial ministry and decided not to intervene. However, if the match becomes routine, the Alberta commissioner will seek a clear statement on the provincial application form telling individuals that the information would be shared with CPP Income Security.

We concluded that HRDC's agreement with Alberta is authorized by both the *Canada Pension Plan Act* and can be argued is consistent with the original use under the *Privacy Act*. However, two further steps need to be taken — particularly if the program is to be expanded to other provinces. HRDC should alert Treasury Board to the new match in the descriptions of its personal information banks in *Info Source*. And HRDC should inform applicants for CPP disability benefits that it will advise provincial income replacement programs of their CPP disability status and benefits.

Notifying Old Age Security of claimants' deaths

Another proposed match will use the Quebec Pension Plan (QPP) database to identify which federal Old Age Security claimants have died. Although HRDC's Income Security Program receives death information from the Quebec vital statistics agencies, the information is not in a standard format and often does not include the SIN. Identifying the correct individual can be difficult.

In all other provinces, residents contribute to the Canada Pension Plan and a death notice to either the OAS or CPP program is communicated to the other. Even though Quebec administers its own plan, heirs and administrators of estates may assume that notifying QPP is sufficient to notify the federal program. This is not so and HRDC has many examples of cheques continuing to be paid after the beneficiary's death.

The match is not yet underway; HRDC is in the final stages of drawing up a data sharing agreement with the Québec Régie des rentes which administers the QPP.

Sharing names of OAS claimants and QPP recipients

A somewhat related match would allow HRDC and QPP to match information about QPP recipients and applicants for Old Age Security, Guaranteed Income Supplement and the Spousal Allowance. Since the federal programs are linked to income, failing to declare income from QPP could give some applicants more than their entitlement.

HRDC ran pilot studies in 1994 and 1996 using the CPP database which identified significant overpayments of the federal benefits to applicants who had misstated or not declared their CPP income. HRDC has no reason to believe that the situation would be any different in Québec but, since it does not have access to QPP data, cannot check.

The match was under consideration at the end of the reporting year.

In the Courts

Reference to the Federal Court by the Privacy Commissioner of Canada and the Attorney General of Canada

Last year's annual report signalled our intention to seek the Court's guidance on the legality of government matching of returning travellers' Customs declarations with the Employment Insurance database. The case has now been filed.

The Court will be asked two questions. The first is whether the *Customs Act* overrides government's obligation in the *Privacy Act* to use personal information only for the purpose for which it is collected, unless the individual consents. The second asks whether searching every returning traveller on suspicion of defrauding Employment Insurance offends the "reasonable search and seizure" provision of the *Canadian Charter of Rights and Freedoms*.

The Office had accepted a pilot project in order for Human Resources Development Canada (HRDC) to gather data for a formal data matching proposal to the Commissioner (required by Treasury Board guidelines). When HRDC moved to implement the project before his review was completed (and without his suggested safeguards), the Commissioner sought legal advice.

The Court will be asked to consider the relationship between the *Customs Act* and the *Privacy Act* by way of a stated case (a statement of facts on which both the Privacy Commissioner and the government agree) under section 17(3) of the Federal Court Act. The question of whether the match offends the Charter is expected to be heard through an appeal of a complainant's case to an umpire under the *Employment Insurance Act*.

The Court is expected to consider the matters this Fall.

Robert Lavigne v. The Office of the Commissioner of Official Languages

The Privacy Commissioner intervened in this application to support Mr. Lavigne's request for access to his personal information. Mr. Lavigne wanted to examine certain witness statements and interview notes contained in the investigative files the Office of the Commissioner of Official Languages compiled while looking into his complaint against Human Resources Development Canada.

Official Languages refused access, arguing that disclosure of this information would harm its enforcement of the *Official Languages Act* (an exemption permitted by s. 22(1)(b) of the *Privacy Act*). Official Languages had relied on provisions in its own legislation — the *Official Languages Act* — which deal with the confidentiality of information obtained during an investigation.

At issue is the proper interpretation of s. 22(1)(b) of the *Privacy Act* and whether the right in the *Privacy Act* to see what others have said about you overrides the confidentiality of investigations under the *Official Languages Act*.

The case will be heard on October 5, 1998.

Privacy Commissioner v. Immigration and Refugee Board

The Privacy Commissioner launched this application with the consent of an individual seeking access to his personal information contained in interview notes. An investigator, hired by the Board to conduct an internal review of several leaks to the media, had interviewed a number of employees and promised them confidentiality.

The Board refused to provide the information to the individual, citing s. 22(1)(b) of the *Privacy Act* (see above). The Board argued that providing access would impede its ability to conduct similar investigations in the future.

In his reasons for judgement released on December 24, 1997, Mr

Justice Richard concluded that the Board “did not have reasonable grounds to withhold disclosure of the records sought in this case”. He held that the Board’s claim of injury was “speculative” and there was “no evidence of probable harm to any investigation that has been undertaken or is about to be undertaken”. He concluded that “one cannot refuse to disclose information under s. 22(1)(b) on the basis that the disclosure will have a chilling effect on possible future investigations”.

He ordered the Board to give the individual the personal information at issue.

The Charter — A Reasonable Expectation of Privacy

In the Beginning

Despite the lack of a specific right to privacy in the *Canadian Charter of Rights and Freedoms*, Canada’s highest Court has recognized privacy as a constitutionally protected or Charter value almost from the beginning.

Several provisions in the Canadian Charter protect privacy values: section 2 protects individuals’ abilities to decide personal beliefs and opinions; section 10, the right to legal counsel; sections 11 and 13, the right against self-incrimination. These rights protect informational privacy by controlling the way information is collected and used. Section 7 provides a right not to be deprived of life, liberty and security of the person, except in accordance with the principles of fundamental justice. This is at least suggestive of privacy protection. But it is section 8 of the Charter — the protection against unreasonable search and seizure — which has been the most valuable for privacy advocates. It’s worth examining some Supreme Court of Canada decisions because they can provide tools for advancing privacy as human right.

Some Key Cases

In *Hunter v. Southam Inc.*¹, the Supreme Court stated that a major purpose of the constitutional protection against unreasonable search and seizure under section 8 of the *Charter of Rights and Freedoms* was the protection of the privacy of the individual. The case involved a constitutional challenge to a search conducted under the *Combines Investigation Act*. The Court concluded that to assess the constitutionality of a search, it must focus on the search's reasonableness or unreasonableness in terms of its impact on the individual and not simply on its rationality in furthering a valid government objective. Mr. Justice Dickson of the Supreme Court advanced in this case for the first time the notion of "reasonable expectation of privacy" as a standard against which government action should be scrutinized. He made it clear that the expectation of privacy was at the forefront of any s. 8 Charter analysis. He said:

"The guarantee of security from unreasonable search and seizure only protects a reasonable expectation. This limitation on the right guaranteed by s. 8 whether it is expressed negatively as freedom from 'unreasonable' search and seizure, or positively as an entitlement to a 'reasonable' expectation of privacy, indicates that an assessment must be made as to whether in a particular situation the public's interest in being left alone by government must give way to the government's interest in intruding on the individual's privacy in order to advance its goals, notably those of law enforcement".

The notion of reasonable expectation of privacy deserves some examination. There is no definition by the Court (or of course, in the Charter). Rather, it is to be determined on the basis of the totality of the circumstances. The American Courts have suggested some guidelines as follows:

- "(i) presence at the time of the search;*
- (ii) possession or control of the property or place searched;*
- (iii) ownership of the property or place;*
- (iv) historical use of the property or item;*

- (v) *the ability to regulate access, including the right to admit or exclude others from the place;*
- (vi) *the existence of a subjective expectation of privacy; and*
- (vii) *the objective reasonableness of the expectation.”*²

These factors are not particularly protective of privacy. The Canadian Court has tended to be more flexible in its approach to what constitutes an unreasonable invasion of privacy. It has found that a person's expectation of privacy is very high in one's own home (but lower in someone else's home) and not so very high in the workplace³; high in hair and saliva samples and teeth impressions but not in the mucous thrown away on a tissue⁴; higher in private phone calls than pay phone calls⁵ and high in private records such as medical or therapeutic records, school records, private diaries⁶. The driver of a vehicle has more expectation of privacy than a passenger and the expectation is higher in a tagged suitcase than a plain garbage bag⁷.

In *R. v. Stewart*⁸, a union seeking to organize hotel employees hired Mr. Stewart to obtain their names, addresses and telephone numbers. Mr. Stewart contacted the hotel security guard and offered to purchase the information. The guard refused, knowing he was not authorized to access that information through the hotel records and that the hotel had previously refused to give the information to the union. Mr. Stewart was charged with counselling to commit fraud and theft. After an acquittal at trial, the Court of Appeal entered a conviction on the charge.

The Supreme Court allowed the appeal on the basis that confidential information does not qualify as property, at least for the purposes of the *Criminal Code* and that Mr. Stewart's conduct did not amount to fraud as it did not involve a risk of economic loss amounting to deprivation. (But that's not the important part.) Cory J.A., as he then was, suggested that information and its collection, collation and interpretation are so vital to modern enterprises that it may be considered their most valuable asset. He then concluded that the confidential or private nature of the information is exactly what gives it its proprietary interest. Picking up on that theme, Mr. Justice Lamer, (now Chief Justice) acknowledged that, "... given recent technological developments, confidential informa-

tion, and in some instances, information of a commercial value, is in need of some protection” but he considered that this was best left to Parliament.

Some six months later, Mr. Justice Lamer had an opportunity to revisit these notions in *R. v. Dyment*⁹. In that case, decided before amendments to the *Criminal Code* dealing with blood samples, a doctor drew a blood sample from an emergency patient without his consent or knowledge in order to provide medical treatment and later gave it to a police officer for his investigation. The sample was used to secure a conviction of impaired driving. Mr. Justice Lamer found that the blood was held by the doctor subject to a duty to respect the patient’s privacy; and Mr. Justice La Forest found that the officer breached the respondent’s privacy interests in the sample and so effected a seizure within the meaning of section 8 of the *Charter of Rights*. This case is often cited for identifying the three types of privacy: physical, territorial and informational. Actually, as the Court pointed out, these categories were first identified in a 1972 joint study by the Federal Department of Justice and the Department of Communications. The Court accepted that the notion of privacy derives from the assumption that all information about a person is in a fundamental way, his own.

Two years later, in *R. v. Duarte*¹⁰, Mr. Justice La Forest had occasion to review the police practice of “consent surveillance” i.e. electronic surveillance without a court authorization where one of the parties to a conversation, an undercover police officer, surreptitiously records it. He reinforced the precept that the Charter standard for privacy is set at a “reasonable expectation of privacy” and that the particular police practice of audio-surveillance failed to meet that standard.

That same year, Mr. Justice LaForest wrote the majority reasons in a case involving unauthorized videotape surveillance of a hotel room. In *R. v. Wong*¹¹, he again stressed the need to interpret the individual’s reasonable expectation of privacy in light of the social importance of privacy. In other words, the question should always be framed in a neutral manner: whether in a society such as ours, persons who retire to a hotel room and close the door have a reasonable expectation of privacy. He considered that the Court must examine the reasonable expectation in the context of a free and democratic society – i.e. without reference to any illegal activity of the particular person.

Mr. Justice Sopinka and Mr. Justice Lamer considered that the Court must evaluate the expectation in light of what a reasonable person placed in those circumstances could expect. For example, in *R. v. Plant*¹², Mr. Justice Sopinka wrote the Court's majority judgment examining the individual's privacy interest in computerized utility records.

In this case, Calgary Police received a tip that an individual was growing marijuana in his house. They searched his electricity records held in the computer of the city's utility commission, using a remote terminal in the police station with a password supplied by the utility. They discovered that the house used four times the average amount of electricity — but typical use for a marijuana operation. Eventually, the owner was charged and convicted. The matter went to the Supreme Court where it was argued that the warrantless search of the owner's computerized records violated his reasonable expectation of privacy under section 8 of the Charter.

The Supreme Court rejected the claim. Justice Sopinka set out five factors for applying the reasonable expectation test: one must consider the nature of the information itself, the nature of the relationship between the party releasing the information and the party claiming its confidentiality, the place where the information was obtained, the manner in which it was obtained, and the seriousness of the crime being investigated. These factors, he felt, would properly allow for a balancing of the societal interest in protecting individual dignity, integrity and autonomy with effective law enforcement. Under the last factor, he concluded that the seriousness of the accused's offence in this case suggested that the accused could not reasonably have a privacy interest which outweighed the state's interest in law enforcement.

In a short but powerful dissent, Madame Justice McLachlin disagreed with the conclusion that police were free to search the database without a warrant. The proper question for her was whether the evidence disclosed a reasonable expectation that the information would be kept in confidence and used only for the purpose for which it was given. Electricity records, she said, were "close to the line" but they deserved protection because they could reveal information about the individual's private life. She writes in her judgment:

“The records are capable of telling much about one’s personal lifestyle, such as how many people lived in the house and what sort of activities were probably taking place there. The records tell a story about what is happening inside a private dwelling, the most private of all places. I think the reasonable person looking at these facts would conclude that the records should be used only for the purpose for which they were made — the delivery and billing for electricity — and not to be divulged to strangers without proper legal authorization.”

In a September 1997 speech entitled “Freedom of Speech and Privacy in the Information Age”, Mr. Justice Sopinka spoke of his approach in the *Plant* case:

“In that case, we had to consider whether it was constitutionally permissible for the police to use its computer records of the electrical consumption at a specified address in order to determine whether or not it was likely that marijuana was being grown at the house, since this is often characterized by a higher than normal consumption of electricity. I observed that the ‘Charter should seek to protect a biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state’. It could be said that information revealing a pattern of electricity consumption would fall into such a category. However, each case must be decided on its own facts, carefully analyzing the extent to which respect for one’s personal privacy and dignity has been violated.”

Justice La Forest has occasionally pursued privacy protection much further than the rest of the Court. In *Edmonton Journal v. Alta (A.G.)*¹³, the Court examined the rights of individuals to protect their privacy against the right of newspapers to report on court proceedings. At issue was a provision of the *Alberta Judicature Act* which limited the publication of information relating to matrimonial cases. In his dissent, Justice La Forest concluded that, although freedom of expression and the need for open courts are important interests, the general publication of details of private family cases serves insufficient public interest and the limitation should stand. Most interestingly, in this case, it was recognized that the privacy of individuals is not only threatened by the

interference of government but also by other powerful entities, such as the media, against which an individual is powerless.

More recently, the Court has extended the notion of privacy into that of reputation, perhaps opening the door to successful claims in damages for invasion of privacy. In *Morris Manning and Church of Scientology of Toronto*¹⁴, Mr. Justice Cory stated:

"..... reputation is intimately related to the right to privacy which has been accorded constitutional protection. As La Forest J. wrote in R. v. Dyment, 'privacy, including informational privacy, is [g]rounded in man's physical and moral autonomy and is essential for the well-being of the individual'. The publication of defamatory comments constitutes an invasion of the individual's personal privacy and is an affront to that person's dignity. The protection of a person's reputation is indeed worthy of protection in our democratic society ..."

For the Future

This notion that the Charter is concerned not only with protecting property but also protecting privacy could be an extremely valuable one. Speaking before the Canadian Human Rights foundation in 1990, Mr. Justice LaForest suggested that "it is with the adoption of section 8 of the Charter that a privacy doctrine has truly developed". However, as Mr. Justice Sopinka has more recently re-iterated on the subject, "... It [the Charter] only applies to government action. Given that much of the world of electronic communication is controlled privately, without any government regulation, the Charter may be an ineffective tool ..."

Several cases could advance to the Supreme Court in which privacy will face off against, not only the historically competing interests like law enforcement, but also those of judicial independence and governance issues. These will test the waters because they raise two interests which the Court has consistently protected. For example, there is what one privacy commissioner describes as a "high technology search and seizure" case. Last year's annual report dealt with the case of the Customs E-311 computer data match. Human Resources Development Canada is matching the Employment Insurance data base with that of returning air travellers custom declarations. The "hit" shows who of

these millions of flyers has been receiving employment insurance payments, possibly undeservedly. The match offends fundamental privacy principles by taking information given by Canadians for one purpose and, without their consent, using it for a very different purpose.

It also violates privacy more fundamentally in that it fails to recognize the right of millions of innocent Canadians to be left alone by their government if they have done nothing wrong. The Privacy Commissioner considers the program violates s. 8 of the Charter in that it erodes Canadians' reasonable expectation of privacy and therefore constitutes an unreasonable search and seizure of personal information. At time of writing, he expects, after months of complex negotiation with the Attorney General, to have the matter before the first level of courts in the Fall of 1998.

1. Hunter et al v. Southam Inc. [1984] 2 S.C.R. 145
2. United States v. Gomez, 16 F.3d 254 (8th Circ. 1994); at p. 256
3. R. v. Silveira [1995] 1 S.C.R. 607; R. v. Edwards [1996] 1 S.C.R. 128
4. R. v. Stillman [1997] 1 S.C.R. 607
5. R. v. Thompson [1990] 2 S.C.R. 1111
6. A. (L.L.) v. B. (A.) [1995] 4 S.C.R. 536;
see also R. v. O'Connor [1995] 4 S.C.R. 411
7. R. v. Belnavis [1997] 3 S.C.R. 341
8. R. v. Stewart [1988] 1 S.C.R. 963
9. R. v. Dyment [1988] 2 S.C.R. 417
10. R. Duarte [1990] 1 S.C.R. 30
11. R. v. Wong [1990] 3 S.C.R. 36
12. R. v. Plant [1993] 3 S.C.R. 281
13. Edmonton Journal v. Alberta (Attorney General) [1989] 2 S.C.R. 1326
14. Hill v. Church of Scientology of Toronto [1995] 2 S.C.R. 1130

Privacy protection in Canada... an update

The following highlights events in the provinces and territories since our last annual report. For a summary of the legal privacy protection in place in each jurisdiction, please check our Web site or call the Office.

Parliament extended Privacy Commissioner Bruce Phillips' term until May 2000. The **federal government** conducted public consultations on a proposed privacy protection law that would apply to the federally-regulated private sector (see page 11).

Alberta renewed Information and Privacy Commissioner Bob Clark's appointment until 2002. As well, the provincial government will extend its *Freedom of Information and Privacy Act* to school boards (effective September 1, 1998), health care bodies (October 1, 1998), universities and colleges (January 4, 1999) and municipal governments and police commissions (October 1, 1999). The government's Health Information Steering Committee, struck by the minister of health, is expected to report in July on a health information act to replace the bill tabled and withdrawn last year. The bill is expected to be debated in the Assembly in February 1999. Finally, the *Freedom of Information and Protection of Privacy Act* will undergo its statutory three-year review this summer.

The **British Columbia** College of Physicians and Surgeons, the B.C. Medical Association and the provincial Information and Privacy Commissioner jointly developed a *Privacy Code* that now protects the confidentiality of personal information held in a doctor's private office. And following an outcry over the intrusiveness of a provincial ministry of human resources consent form, the Commissioner's office reviewed and advised on a replacement form and pamphlet (see page 82). The Commissioner's office also reviewed a College of Pharmacists' audit and inspection reports on use of Pharmanet, the province's on-line drug prescription and billing system.

Manitoba adopted two new laws to protect Manitobans' privacy. The new *Freedom of Information and Protection of Privacy Act*, proclaimed in May 1998, replaces the 1988 *Freedom of Information Act* and expands provincial residents' privacy rights to include controls on government bodies' collection, use and disclosure of their personal data. As well, effective December 1997, the *Personal Health Information Act* (the first

such law in Canada), regulates the collection, use and disclosure of medical records. Both laws are overseen by provincial Ombudsman Barry Tuckett who has appointed former provincial archivist Peter Bower as executive director of the office's new Freedom of Information and Protection of Privacy Division.

New Brunswick passed its new *Protection of Personal Information Act* February 1998 (the law is not yet in force). The new Act applies to the provincial public sector and is the first in Canada based on the Canadian Standards Association's Model Privacy Code. Responsibility for oversight was given to the provincial Ombudsman. In addition, the provincial justice minister announced his intention to "present a discussion paper soon considering the possible extension of privacy legislation to the private sector". Public consultations are scheduled to take place in the summer of 1998.

Despite calls for revamping the provincial *Privacy Act* (a tort law), **Newfoundland and Labrador** have made only minor amendments to that statute, and to the province's *Freedom of Information Act*, dealing with the disclosure of a person's criminal history.

Several **Ontario** initiatives will have an impact on individuals' privacy. Students will now be assigned a unique ID number which will be used in place of their names to allow the Ministry of Education to track them throughout their schooling. New regulations will now impose certain restrictions on the search powers which currently allow social workers to search a welfare recipient's house to verify eligibility. And social assistance recipients must now be identified using a biometric identifier — a digitized fingerprint. The provincial government is also working on a proposed *Personal Health Information Protection Act* that would regulate the collection, use and disclosure of medical information, which the government announced would pave the way to equip every Ontarian with a smart health card. The bill may be tabled in 1998. And finally, the Legislature appointed former Assistant Privacy Commissioner Ann Cavoukian to replace outgoing Information and Privacy Commissioner Tom Wright who completed his term in April 1997.

Prince Edward Island remains the only province without privacy legislation. However, the government tabled a proposed *Freedom of Information and Protection of Privacy Act* (Bill 81) in November 1997, which awaits second reading in the Legislature.

In the Fall of 1997, **Québec's** National Assembly conducted public consultations on amendments to the province's two key privacy protection statutes; the 16-year old law governing the public sector, and the five-year old law regulating private business. The National Assembly also tabled its final report on a provincial identity or multi-purpose card, recommending that no card be developed now for lack of a demonstrated need. However, it suggested that the government might consider an optional identification card for those wanting one. The provincial Privacy Commission embarked on a thorough review of the security and confidentiality mechanisms protecting provincial government databases in reaction to the well-publicized improper sale of Quebecers' personal information by civil servants (who were later fired). As well, the Commission continues seeking controls on the extraordinary powers given to the provincial revenue ministry which, to wage its war against tax fraud, has been armed with the unchallenged right to access any personal information held by any public sector agency.

Corporate Management

The Privacy and Information Commissioners share premises and administrative services while operating separately under their statutory authorities. These shared services — finance, personnel, information technology and general administration — are centralized in Corporate Management Branch to avoid duplication of effort and to save money for both government and the programs. The Branch has just 14 staff and a budget representing 14 per cent of total program expenditures.

Resource Information

The Offices' total budget for the 1997-98 fiscal year was \$6,616,000. Actual expenditures for 1997-98 were \$6,440,099 of which, personnel costs of \$5,308,203 and professional and special services expenditures of \$695,181 accounted for more that 93 per cent of all expenditures. The remaining \$436,715 covered all other expenditures including postage, telephone, office equipment and supplies.

Expenditure details are reflected in Figure 1 (resources by organization/activity) and Figure 2 (details by object of expenditure).

Figure 1
1997-98 Resources by Organization/Activity

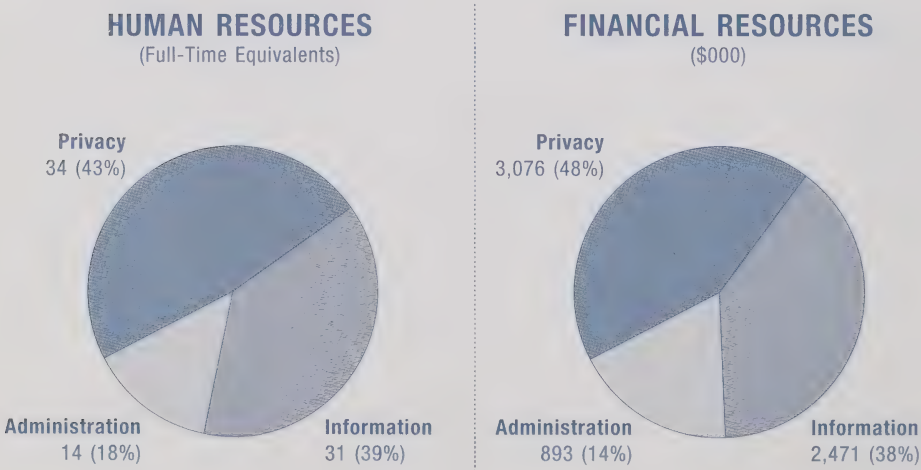
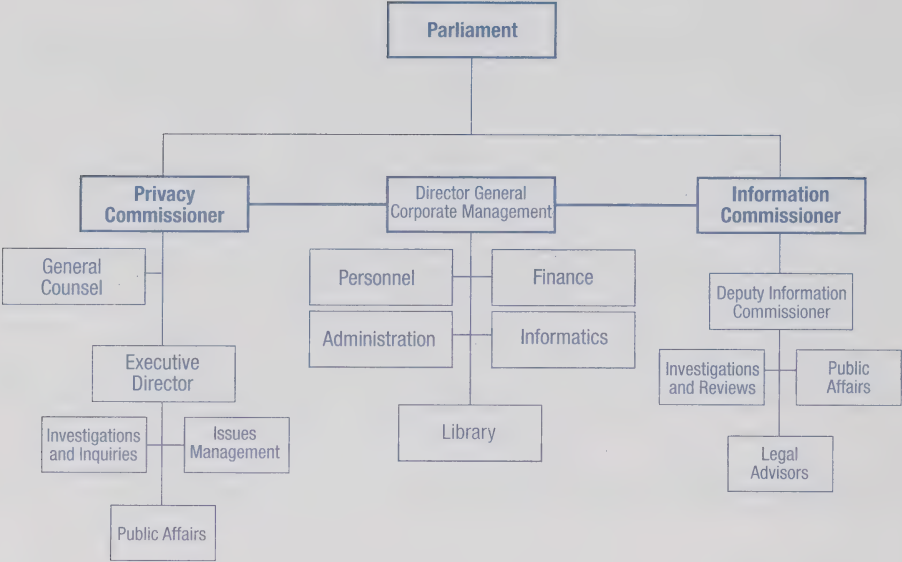


Figure 2
Details by Object of Expenditure

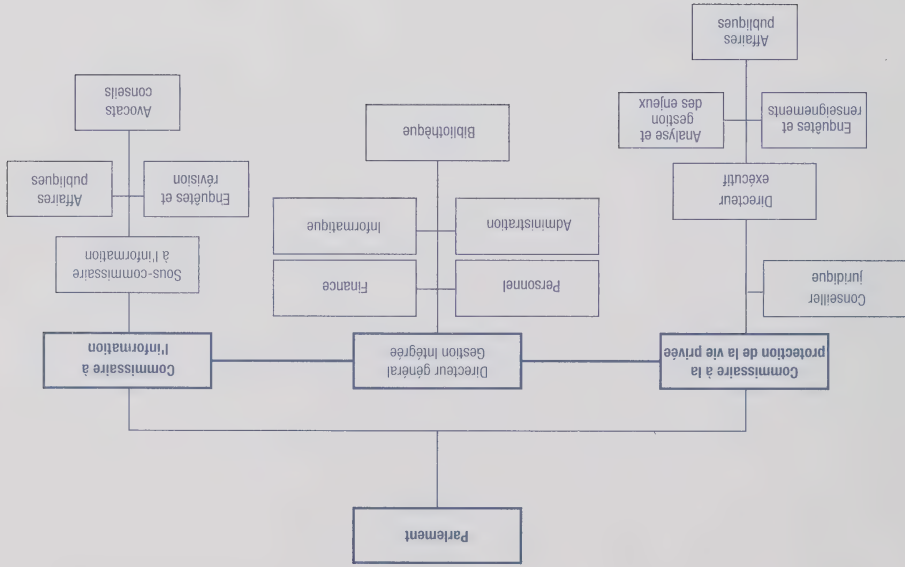
	Information	Privacy	Corporate Management	Total
Salaries	1,829,617	2,092,930	576,656	4,499,203
Employee Benefit Plan Contributions	323,000	378,000	108,000	809,000
Transportation and Communication	48,389	62,656	99,186	210,231
Information	24,524	36,916	2,212	63,652
Professional and Special Services	181,559	463,334	50,288	695,181
Rentals	16,359	715	15,043	32,117
Purchased Repair and Maintenance	3,110	5,898	8,113	17,121
Utilities, Materials and Supplies	26,388	12,498	29,088	67,974
Acquisition of Machinery and Equipment	17,643	22,932	4,825	45,400
Other Payments	125	95	-	220
Total	2,470,714	3,075,974	893,411	6,440,099

* Expenditure Figures do not incorporate final year-end adjustments reflected in the Offices' 1997-98 Public Accounts.

Organization Chart



Organigramme



Ventilation par article de dépense

Tableau 2

	Information	Vie privée	Gestion Intégrée	Total
Salaires	1,829,617	2,092,930	576,656	4,499,203
Contributions aux régimes d'avantages sociaux	323,000	378,000	108,000	809,000
Transports et communications	48,389	62,656	99,186	210,231
Information	24,524	36,916	2,212	63,652
Services professionnels et spéciaux	181,559	463,334	50,288	695,181
Locations	16,359	715	15,043	32,117
Achat de services et réparations	3,110	5,898	8,113	17,121
Services publics, approvisionnements, fournitures	26,388	12,498	29,088	67,974
Achat de machines et d'équipement	17,643	22,932	4,825	45,400
Autres paiements	125	95	-	220
Total	2,470,714	3,075,974	893,411	6,440,099

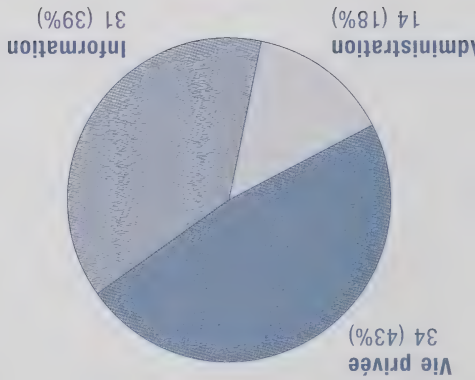
* Ces dépenses ne reflètent pas les rajustements de fin d'exercice indiqués aux Comptes publics des Commissariats pour 1997-1998.

1997-98 Ventilation par organismes/activités

Tableau 1

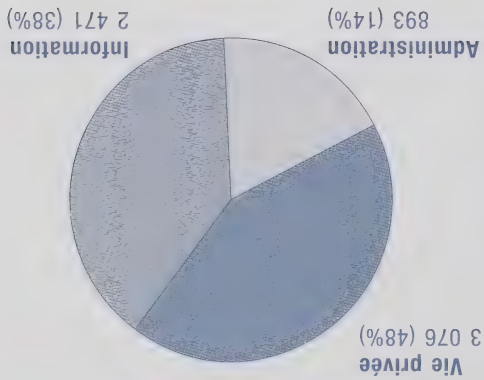
RESSOURCES HUMAINES

(équivalents temps plein)



RESSOURCES FINANCIÈRES

(en milliers de \$)



Direction de la gestion intégrée

Même s'ils partagent locaux et services administratifs, le Commissariat à la protection de la vie privée et le Commissariat à l'information fonctionnent de façon indépendante en vertu des lois habilitant leurs opérations. Par souci d'économie et d'efficacité pour le gouvernement et les programmes, ces services, (finances, personnel, soutien informatique et administration générale) sont centralisés dans la Direction de la gestion intégrée. La direction compte un personnel de quatorze personnes seulement et un budget qui représente environ 14 p. 100 du budget total des dépenses de tout le programme.

Description des ressources

Le budget combiné que les deux Commissariats avaient projeté pour l'exercice 1997-1998 s'élevait à 6 616 000 \$. Les dépenses réelles pour l'exercice 1997-1998 étaient de 6 440 099 \$. De cette somme, 5 308 203 \$ ont été affectés au personnel et 695 181 \$ ont été versés en services professionnels spéciaux (contractuels et conseillers juridiques de l'extérieur), soit 93 pour cent de toutes les dépenses. Le solde de 436 715 \$ a été affecté à tous les autres coûts, y compris la poste, les télécommunications, les fournitures et l'équipement de bureau.

Les dépenses sont ventilées au tableau 1 (Ressources par organismes/activités), et au tableau 2 (Ventilation par article de dépense).

digitales. Le gouvernement provincial élabore maintenant une loi qui réglementerait la collecte, l'utilisation et la communication des renseignements médicaux et qui doterait, semble-t-il, chaque Ontarien d'une carte à puce. Le projet de loi devrait être déposé en 1998. L'Assemblée législative de l'Ontario a nommé l'ancienne commissaire adjointe à la vie privée, Mme Ann Cavoukian, au poste de commissaire à l'Information et à la protection de la vie privée; le mandat de l'ancien commissaire a pris fin en avril 1997.

L'Ile-du-Prince-Édouard demeure la seule province sans loi sur la protection des renseignements personnels. Toutefois, en novembre 1997, le gouvernement a déposé le projet de loi 81 sur le *Freedom of Information and Protection of Privacy Act* qui attend d'être débattu en deuxième lecture.

À l'automne 1997, l'Assemblée nationale du **Québec** a mené des consultations publiques sur les modifications à apporter aux deux lois principales sur la protection de la vie privée, soit la loi vieille de seize ans qui s'applique au secteur public, et celle vieille de cinq ans qui s'applique au secteur privé. L'Assemblée a aussi déposé son rapport final sur une carte d'identité provinciale ou multi-services dans lequel on recommande qu'aucune carte ne soit développée puisqu'on n'est pas parvenu à en démontrer l'utilité. Cependant, on envisage d'émettre une carte d'identification facultative à qui la voudrait. La Commission d'accès à l'information a entrepris un examen approfondi des mécanismes de protection de la confidentialité des renseignements contenus dans les bases de données, en réaction à la vente de renseignements personnels par des fonctionnaires (congelés par la suite), qui a fait couler beaucoup d'encre. En outre, la Commission continue de chercher à faire appliquer des mesures de contrôle relativement aux pouvoirs extraordinaires conférés au ministère du Revenu de la province, lequel a été doté, pour la chasse aux fraudeurs, d'un droit d'accès non contestable à tous les renseignements personnels détenus par un organisme public.

Le **Manitoba** a adopté deux nouvelles lois afin de protéger la vie privée des Manitobains. La nouvelle *Loi sur l'accès à l'information et la protection de la vie privée* a remplacé en 1998 la *Loi sur la liberté d'accès à l'information* de 1988; elle élargit les droits accordés aux résidents, et comprend des mesures de réglementation sur la collecte, l'utilisation et la communication de leurs renseignements personnels par des organismes gouvernementaux. En outre, depuis décembre 1997, la *Loi sur les renseignements médicaux personnels* (première loi du genre au Canada) réglemente la collecte, l'utilisation et la communication des dossiers médicaux. Ces deux lois sont administrées par l'Ombudsman du Manitoba, M. Barry Tuckett; ce dernier a nommé l'ancien archiviste provincial, M. Peter Bower, au poste de directeur exécutif de la nouvelle Division de l'accès à l'information et de la protection de la vie privée.

Le **Nouveau-Brunswick** a adopté en février 1998 la *Loi sur la protection des renseignements personnels*, qui n'est pas encore entrée en vigueur. Cette loi, qui s'appliquera au secteur public provincial, est la première loi fondée sur le code modèle de la vie privée qu'a proposé l'Association canadienne de normalisation. L'Ombudsman provincial s'est vu accorder un droit de regard. En outre, le ministre de la Justice de la province a fait part de son intention de présenter bientôt un document de travail envisageant d'étendre au secteur privé la législation sur la vie privée. Des consultations publiques devraient avoir lieu à l'été 1998.

À **Terre-Neuve et au Labrador**, la *Privacy Act* et la *Freedom of Information Act* n'ont subi que des modifications mineures sur la communication des dossiers criminels, bien qu'il ait été préconisé de les reformuler.

En **Ontario**, plusieurs initiatives auront une influence importante sur la vie privée. L'étudiant aura maintenant un numéro d'identification unique qui le suivra pendant toutes ses études. Un travailleur social peut fouiller la résidence d'un prestataire de l'aide sociale à des fins de vérification de l'admissibilité. Pour sa part, l'assisté social doit maintenant être identifié par un code biométrique ou ses empreintes

Mise à jour sur la protection de la vie privée au Canada

Les rubriques illustrent les événements survenus dans les provinces et les territoires depuis notre dernier rapport annuel. Pour consulter un résumé des mesures de protection juridiques en place dans chaque administration, veuillez visiter notre site Web ou communiquer avec notre bureau.

Le **Parlement** a prolongé le mandat du Commissaire à la protection de la vie privée jusqu'en mai 2000. Le **gouvernement fédéral** a mené des consultations publiques sur la loi envisagée pour protéger la vie privée dans le secteur privé sous réglementation fédérale (voir la page 12).

L'**Alberta** a renouvelé le mandat du Commissaire à l'information et à la protection de la vie privée, M. Robert Clark, jusqu'en 2002. Il a aussi étendu sa loi sur l'accès à l'information et la protection de la vie privée aux conseils scolaires (à compter du 1^{er} septembre 1998), aux organismes de soins de santé (1^{er} octobre 1998), aux collèges et universités (4 janvier 1999) et aux gouvernements municipaux ainsi qu'aux corps policiers (1^{er} octobre 1999). Le *Health Information Steering Committee* du gouvernement, établi par le ministre de la Santé, doit déposer son rapport en juillet sur un projet de loi sur la santé visant à remplacer celui qui a été déposé, puis retiré l'an dernier. Le projet de loi doit être débattu par l'Assemblée en février 1999. En dernier lieu, la *Freedom of Information and Protection of Privacy Act* subira son examen triennal obligatoire cet été.

En **Colombie-Britannique**, le *College of Physicians and Surgeons*, l'Association médicale de la C.B. et le Commissaire à l'information et la vie privée de la C.B. ont développé un *code de la vie privée* qui protège la confidentialité des renseignements personnels confiés au médecin dans son bureau privé. Suite au tollé général soulevé par le formulaire de consentement du ministère des Ressources humaines de la province, le bureau du commissaire a revu et proposé un formulaire de remplacement ainsi qu'une brochure (voir la page 90). Il a également revu la vérification menée au Collège des pharmaciens ainsi que les rapports d'inspection sur l'utilisation de Pharmanet, le système d'ordonnances et de facturation en direct.

1. Hunter et al c. Southam Inc. [1984] 2 R.C.S. 145
2. United States c. Gomez, 16 F.3d 254 (8th Circ. 1994), at p. 256
3. R. c. Silveira [1995] 1 R.C.S. 607; R. c. Edwards [1996] 1 R.C.S. 128
4. R. c. Stillman [1997] 1 R.C.S. 607
5. R. c. Thompson [1990] 2 R.C.S. 1111
6. A. (L.L.) c. B. (A.) [1995] 4 R.C.S. 536;
voir aussi R. c. O'Connor [1995] 4 R.C.S. 411
7. R. c. Belnavis [1997] 3 R.C.S. 341
8. R. c. Stewart [1988] 1 R.C.S. 963
9. R. c. Dymment [1988] 2 R.C.S. 417
10. R. Duarte [1990] 1 R.C.S. 30
11. R. c. Wong [1990] 3 R.C.S. 36
12. R. c. Plant [1993] 3 R.C.S. 281
13. Edmonton Journal c. Alberta (Procureur général) [1989] 2 R.C.S. 1326
14. Hill c. Eglise de scientologie de Toronto [1995] 2 R.C.S. 1130

Cette notion selon laquelle la Charte se préoccupe de protéger, non seulement la propriété, mais aussi la vie privée pourrait être une notion extrêmement précieuse. Lorsqu'il a pris la parole devant la Fondation canadienne des droits de la personne en 1990, le juge La Forest a suggéré que c'est avec l'adoption de l'article 8 de la Charte qu'une doctrine de vie privée s'est réellement développée. Toutefois, comme l'a réitéré plus récemment le juge Sopinka, la Charte s'applique seulement à l'action gouvernementale; étant donné qu'une grande partie du monde de la communication électronique est sous le contrôle du secteur privé, sans réglementation gouvernementale, la Charte peut être un outil inefficace.

Il doit exister un certain nombre de causes qui pourraient être portées devant la Cour suprême où la vie privée sera carrément confrontée à des intérêts contraires établis de longue date, comme l'application de la loi, et aussi ceux de l'indépendance judiciaire et l'exercice de l'autorité. Ces causes permettront de se faire une idée de la situation parce qu'elle soulèvent deux intérêts que la Cour a protégés de façon constante. Par exemple, il y a ce qu'un commissaire à la vie privée décrit comme une cause de fouilles, perquisitions et saisies à l'aide de technologie de pointe. Le rapport annuel de l'an dernier traitait du cas de couplage des données informatisées E-311 des Douanes. Développement des ressources humaines Canada couple la base de données de

L'assurance-emploi et les déclarations de douane des voyageurs rentrant au pays par avion, pour savoir lesquels, sur ces millions de voyageurs, ont reçu des prestations d'assurance-emploi, peut-être de façon induc.

Le couplage enfreint les principes fondamentaux de vie privée en prenant les renseignements offerts par les Canadiens à une fin et en les utilisant, à leur insu et sans leur consentement, à une fin très différente. Ce couplage enfreint aussi la vie privée de façon encore plus fonda-

mentale parce qu'il nie le droit de millions de Canadiens innocents à ne pas subir l'ingérence de leur gouvernement s'ils n'ont rien fait de mal. Le Commissaire à la vie privée juge que le programme enfreint l'article 8 de la Charte en ce sens qu'il érode l'attente raisonnable de respect de la vie privée des Canadiens et, par là, constitue une fouille ou une saisie abusive de renseignements personnels. Au moment de la rédaction du présent rapport, on s'attend à ce qu'après des mois de négociation complexe avec le Procureur général, la question soit portée en première instance en mai 1998.

ratique, vouloir constituer et soustraire à la connaissance de l'État". On pourrait dire que les renseignements indicatifs de la consommation d'électricité relèverait de cette catégorie. Toutefois, chaque cas doit être décidé d'après ses propres faits, après une analyse soigneuse de la mesure dans laquelle le respect de la vie privée et de la dignité personnelles a été enfreint. »

À l'occasion, le juge La Forest a été bien plus loin dans la poursuite de la protection de la vie privée que ne l'a fait le reste des juges de la Cour. Dans la cause *Edmonton Journal c. Alta (A.G.)*¹³, la Cour a examiné les droits des personnes de protéger leur vie privée par rapport au droit des journaux de commenter les procédures judiciaires. Le litige concernait une disposition de la *Alberta Judicature Act* qui limite la publication des renseignements concernant les instances matrimoniales. Dans son opinion dissidente, le juge La Forest a conclu que, même si la liberté d'expression et le besoin de transparence relativement au fonctionnement des tribunaux sont des intérêts importants, la publication générale des détails des causes familiales privées sert un intérêt public insuffisant, et la limitation devrait être maintenue. Le plus intéressant, dans cette cause, c'est qu'il a été reconnu que la vie privée peut être lésée, non seulement par l'ingérence du gouvernement, mais aussi par d'autres entités puissantes, comme les médias, contre lesquelles une personne est impuissante.

Plus récemment, la Cour a étendu la notion de vie privée à celle de la réputation, ce qui ouvre peut-être la porte à des réclamations en dommages-intérêts pour invasion de la vie privée. Dans la cause *Morris Manning and Church of Scientology of Toronto*¹⁴, le juge Cory a déclaré :

«...En outre, la réputation est étroitement liée au droit à la vie privée, qui jouit d'une protection constitutionnelle. Comme le juge La Forest le dit dans R. c. Dymment, [1988] 2 R.C.S. 417, à la p. 427, la vie privée, y compris la vie privée sur le plan de l'information, est fondée sur l'autonomie morale et physique de la personne et "est essentielle à son bien-être". La publication de commentaires diffamatoires constitue une intrusion dans la vie privée d'un individu et un affront à sa dignité. La réputation d'une personne mérite effectivement d'être protégée dans notre société démocratique ...»

« Dans cette cause, nous avons eu à examiner la question de savoir si, du point de vue constitutionnel, la police est autorisée à utiliser les dossiers de consommation d'électricité d'une adresse particulière pour établir si du chanvre indien est cultivé dans la maison, puisque la culture du chanvre indien est sou-vent caractérisée par une consommation d'électricité plus élevée que la normale. J'ai fait observer que "la Charte protège un ensemble de renseignements biographiques d'ordre personnel que les particuliers pourraient, dans une société libre et démoc-

[TRANSDUCTION]

Dans un discours prononcé en septembre 1977, intitulé *Freedom of Speech and Privacy in the Information Age*, le juge Sopinka a parlé de son approche dans la cause *Plant*. Il a dit à l'audience :

« Il est possible de tirer des dossiers en cause beaucoup de renseignements sur le mode de vie d'une personne et sur ce qui se passe à l'intérieur du lieu privé par excellence qu'est une habitation privée. Une personne raisonnable serait amenée à conclure que les dossiers ne devraient servir qu'aux fins pour lesquelles ils ont été constitués et qu'ils ne devraient pas être mis à la disposition de n'importe qui sans l'autorisation judici-

aire voulue. »

personne. Elle écrit dans son jugement :

d'être protégés parce qu'ils pouvaient renseigner sur la vie privée de la consommation d'électricité étaient un « cas limite », mais ils méritaient fins pour lesquelles ils avaient été constitués. À son avis, les dossiers de renseignements demeureraient confidentiels et serviraient seulement aux de savoir si la preuve indiquait une attente raisonnable que les ren-

avoir de mandat. À ses yeux, la question primordiale qui se posait était conclu que la police n'était pas libre de fouiller la base de données sans Dans une courte, mais puissante opinion dissidente, la juge McLachlin a

maît.

protégée parce que l'intérêt de l'État dans l'application de la loi pri-cusé ne pouvait s'attendre raisonnablement à ce que sa vie privée soit crime, il a conclu que la gravité du délit dans ce cas suggérerait que l'ac-de la loi. Pour ce qui est de la dernière considération, soit la gravité du l'intégrité et l'autonomie de la personne – et une application efficace

sonne à la lumière de l'importance sociale de la vie privée. En d'autres termes, la question devrait plutôt être posée en termes plus neutres de sorte que l'on se demande si, dans une société comme la nôtre, les personnes qui se retirent dans une chambre d'hôtel et qui ferment la porte derrière elles peuvent raisonnablement s'attendre au respect de leur vie privée. Il jugeait que la Cour doit tenir compte de l'attente raisonnable dans le contexte d'une société libre et démocratique – c.-à-d. sans faire renvoi à une activité illégale de la personne concernée.

Le juge Sopinka, d'autre part, et aussi le juge Lamer, semblent penser que la Cour doit évaluer cette attente à la lumière de ce à quoi une personne raisonnable, placée dans ces circonstances, pourrait s'attendre. Par exemple, dans la cause **R. c. Plant**¹², le juge Sopinka a rédigé le jugement rendu à la majorité de la Cour, qui examinait l'intérêt de vie privée d'une personne dans les dossiers informatisés d'un service public. Il a établi cinq considérations que la Cour utiliserait pour déterminer si l'attente de respect de la vie privée d'une personne avait été enfreinte.

Dans cette cause, le service de police de Calgary avait reçu une information selon laquelle une personne cultivait du chanvre indien dans sa maison. Les policiers ont consulté le dossier de consommation d'électricité de la personne en interrogeant, à partir d'un terminal du poste de police et d'un mot de passe que leur avait remis le service public, l'ordinateur du service d'électricité de la ville. Ils ont ainsi découvert que la maison consommait quatre fois plus d'électricité que la moyenne, mais typique pour cultiver le chanvre indien. Le propriétaire a par la suite été accusé et reconnu coupable, et la question a été portée devant la Cour suprême, où il a été soutenu que la fouille sans mandat du dossier informatisé du propriétaire enfreignait l'attente raisonnable de respect de la vie privée de ce dernier aux termes de l'article 8 de la Charte.

La Cour suprême a rejeté cette assertion. Le juge Sopinka a énoncé les facteurs à considérer pour l'application du critère de l'attente raisonnable : la nature des données, de la relation existant entre l'accusé et le service d'électricité, l'endroit où a eu lieu la perquisition et les conditions dans lesquelles elle a été effectuée, ainsi que de la gravité de l'infraction faisant l'objet de l'enquête. Selon lui, ces considérations permettraient de concilier l'intérêt de la société – protéger la dignité,

les renseignements à valeur commerciale devraient être protégés, mais il jugeait que la question était avant tout du ressort du Parlement.

Quelque six mois plus tard, le juge Lamer a eu l'occasion de revoir ces notions dans la cause **R. Dymment**. Dans cette cause, jugée avant que le *Code criminel* ne soit modifié en ce qui a trait aux prélèvements sanguins, un docteur a prélevé du sang d'un patient à l'urgence, sans son consentement ou sa connaissance, pour fournir un traitement médical, et il a ultérieurement remis le prélèvement à un agent de police pour son enquête. Le prélèvement a servi à obtenir une condamnation de conduite en état d'ivresse. Le juge Lamer a conclu que le médecin détenait le prélèvement sanguin sous réserve de son devoir de respecter la vie privée du patient; et le juge La Forest a conclu que l'agent avait enfreint les intérêts de vie privée de l'intime dans le prélèvement et, par là, effectué une saisie abusive au sens de l'article 8 de la *Charte*.

Cette cause est souvent citée parce qu'elle relève trois catégories de vie privée : physique, spatiale et informationnelle. Dans les faits, comme l'a souligné la Cour, ces catégories ont été relevées pour la première fois dans une étude de 1972 menée conjointement par les ministères fédéraux de la Justice et des Communications. La Cour a accepté que la notion de vie privée tire son origine de l'hypothèse selon laquelle tous les renseignements au sujet d'une personne lui appartiennent d'une manière fondamentale.

Deux ans plus tard, dans la cause **R. c. Duarte**¹⁰, le juge La Forest a eu l'occasion d'examiner la méthode policière de la surveillance participative, c.-à-d. la surveillance électronique effectuée sans autorisation, où l'un des participants à une conversation, soit l'agent d'infiltration, enregistre subrepticement la conversation. Il a renforcé le précepte voulant que la norme de vie privée selon la Charte est établie comme policière de l'écoute subreptice des conversations ne respectait pas cette norme.

Durant l'année où était entendue la cause *Duarte*, le juge La Forest a rédigé les motifs de la majorité dans un affaire mettant en cause la surveillance magnétoscopique effectuée subrepticement dans une chambre d'hôtel. Dans la cause **R. c. Wong**¹¹, il a de nouveau souligné le besoin d'interpréter l'attente raisonnable de respect de la vie privée d'une per-

Ces facteurs ne sont pas particulièrement protecteurs de la vie privée. La Cour canadienne a eu tendance à être plus souple dans son approche face à ce qui constitue une invasion abusive de la vie privée. Elle a conclu qu'une personne s'attend à ce que sa vie privée soit fortement respectée dans sa propre maison (mais moins dans la maison d'une autre personne) et pas très respectée à son lieu de travail³, fortement lorsqu'il s'agit de prélèvements de cheveux et de salive, ainsi que les empreintes dentaires, mais moins lorsqu'il s'agit de mucosités rejetées dans un papier-mouchoir⁴; plus lorsqu'il s'agit d'appels privés que d'appels placés par un téléphone public⁵ et plus lorsqu'il s'agit de dossiers privés, comme les dossiers médicaux ou thérapeutiques, dossiers scolaires, journaux intimes⁶. Le conducteur d'un véhicule s'attend à ce que sa vie privée soit davantage respectée qu'un passager; de même pour une valise étiquetée qu'un simple sac à ordures⁷.

Dans **R. c. Stewart**⁸, un syndicat qui cherchait à mobiliser les employés d'un hôtel a embauché M. Stewart pour obtenir les noms, adresses et numéros de téléphone des employés de l'hôtel. M. Stewart a contacté le garde de sécurité de l'hôtel et a offert d'acheter les renseignements. Le garde a refusé parce qu'il savait qu'il n'était pas autorisé à avoir accès aux renseignements figurant dans les dossiers de l'hôtel, et que l'hôtel avait déjà refusé de les remettre au syndicat. M. Stewart a été accusé d'encourager la perpétration de fraude et de vol. Il a été acquitté au procès, mais la Cour d'appel l'a déclaré coupable à l'égard de cette accusation.

La Cour suprême a accepté l'appel en soutenant que des renseignements confidentiels ne peuvent être considérés comme un bien, au moins aux fins du *Code criminel*, et que la conduite de M. Stewart ne constituait pas de la fraude parce qu'il n'y avait pas de danger de pertes économiques constituant une dépossession. (Mais cela n'est pas le plus important.) Le juge Cory a suggéré que les renseignements ainsi que leur collecte, leur regroupement et leur interprétation sont si essentiels aux entreprises modernes qu'on peut les considérer comme leur bien le plus utile. Il a alors conclu que la nature confidentielle ou privée des renseignements est exactement ce qui leur confère leur intérêt en propre. Reprenant ce thème, le juge Lamer de la Cour suprême (il est maintenant juge en chef) a reconnu que, compte tenu de l'essor récent de la technologie, les renseignements confidentiels et, dans certains cas,

notion de l'attente raisonnable de respect de la vie privée comme norme par rapport à laquelle un acte du gouvernement devrait être examiné soigneusement. Il a précisé que l'attente de respect de la vie privée était au premier plan de toute analyse de l'article 8 de la Charte. Il a déclaré :

« La garantie de protection contre les fouilles, les perquisitions et les saisies abusives ne vise qu'une attente raisonnable. Cette limitation du droit garanti par l'art. 8, qu'elle soit exprimée sous la forme négative, c'est-à-dire comme une protection contre les fouilles, les perquisitions et les saisies «abusives», ou sous la forme positive comme le droit de s'attendre «raisonnablement» à la protection de la vie privée, indique qu'il faut apprécier si, dans une situation donnée, le droit du public de ne pas être importuné par le gouvernement doit céder le pas au droit du gouvernement de s'immiscer dans la vie privée des particuliers afin de réaliser ses fins et, notamment, d'assurer l'application de la loi. »

La notion d'attente raisonnable de respect de la vie privée mérite qu'on s'y attarde. Elle n'est pas définie par la Cour (ni, bien sûr, dans la Charte). On doit plutôt l'établir sur la base de l'ensemble des circonstances. Les tribunaux américains ont suggéré certaines lignes directrices, comme suit :

[TRADUCTION]

- « (i) la présence au moment de la fouille;
- (ii) la possession ou le contrôle du bien ou de l'endroit faisant l'objet de la fouille;
- (iii) la propriété du bien ou de l'endroit;
- (iv) l'utilisation historique du bien ou de l'article;
- (v) la capacité de réglementer l'accès, y compris le droit d'admettre ou d'exclure d'autres personnes de l'endroit;
- (vi) l'existence d'une attente subjective de respect de la vie privée;
- (vii) le caractère raisonnable et objectif de l'attente. » ²

La Charte - une attente raisonnable de respect de vie privée

Dans un premier temps

Même si la *Charte canadienne des droits et libertés* n'enchâsse pas de droit particulier au respect de la vie privée, la plus haute cour du Canada a reconnu la vie privée comme étant constitutionnellement protégée ou représentant une valeur selon la Charte presque dès le début.

Diverses dispositions de la Charte protègent les valeurs de vie privée. L'article 2 protège les libertés fondamentales en matière de liberté de conscience et de religion; l'article 10, le recours à un avocat; les articles 11 et 13, le droit contre l'auto-incrimination. Tous ces droits protègent les renseignements personnels en réglementant la façon dont ils sont recueillis et utilisés. L'article 7 prévoit que chacun a droit à la vie, à la liberté et à la sécurité de sa personne, et qu'il ne peut être porté atteinte à ce droit qu'en conformité avec les principes de justice fondamentale. Cela est à tout le moins évocateur de la protection de la vie privée. Toutefois, c'est l'article 8 de la Charte – la protection contre les fouilles, les perquisitions ou les saisies abusives – qui a été la plus précieuse pour les défenseurs de la vie privée. Les décisions de la Cour suprême du Canada constituent à cet égard des outils pour faire progresser la vie privée comme droit de la personne.

Quelques causes clés

Dans **Hunter c. Southam Inc.**¹, la Cour suprême a déclaré qu'un but majeur de la protection constitutionnelle contre les fouilles, les perquisitions ou les saisies abusives aux termes de l'article 8 de la *Charte* est de protéger la vie privée. La cause comportait une action avec contestation de la constitutionnalité d'une fouille effectuée aux termes de la *Loi relative aux enquêtes sur les coalitions*. La Cour a conclu que, pour évaluer la constitutionnalité de la fouille, elle devait s'interroger sur le caractère raisonnable ou abusif de la fouille en termes de son impact sur la personne, et non du simple fait qu'elle apparaissait justifiée pour l'avancement d'un objectif valide du gouvernement. Le juge Dickson de la Cour suprême a proposé dans cette cause, pour la première fois, la

La Commission a refusé de fournir les renseignements en s'appuyant sur l'alinéa 22(1)b) de la Loi sur la protection des renseignements personnels. Elle a soutenu que le fait de donner accès aux renseignements demandés serait préjudiciable à sa capacité de mener d'autres enquêtes similaires dans l'avenir.

Dans son jugement du 24 décembre 1997, le juge Richard a conclu que la Commission n'avait pas de motif raisonnable de ne pas communiquer les renseignements demandés. Il a soutenu que l'assertion de préjudice était de nature spéculative et qu'il n'y avait aucune preuve de dommage probable à toute enquête passée ou future. Il a conclu qu'on ne peut refuser l'accès aux termes de l'alinéa 22(1)b) en prétextant que la communication aurait un effet dissuasif sur les enquêtes futures. Il a ordonné qu'on communique à la personne ses renseignements personnels.

Robert Lavigne c. le Commissaire aux langues officielles

Le Commissaire à la protection de la vie privée est intervenu à l'appui d'une requête de M. Lavigne pour l'accès à ses renseignements personnels. Ce dernier voulait consulter des déclarations et notes d'entrevues de témoins contenues dans des dossiers d'enquête compilés par le Commissaire aux langues officielles dans le cadre d'une enquête sur la plainte qu'il avait déposée contre IDRHC.

Le refus du Commissariat aux langues officielles était basé sur le fait que la communication de ces données serait préjudiciable à l'application de la *Loi sur les langues officielles* parce qu'elle s'était appuyée sur les dispositions de cette loi en matière de confidentialité des renseignements obtenus au cours d'une enquête (les dispositions de la Loi sur les langues officielles prévalent sur celles de la *Loi sur la protection des renseignements personnels* selon l'alinéa 22(1)b) de cette dernière).

L'interprétation convenable de cette dernière disposition était cruciale, ainsi que la question de savoir si le droit de voir ce que les autres disent à notre propos prévaudrait sur la confidentialité des enquêtes menées en vertu de la *Loi sur les langues officielles*.

Le cas sera entendu en cour le 5 octobre 1998.

Le Commissaire à la protection de la vie privée c. Immigration et la Commission du statut de réfugié

Cette requête a été entreprise par le Commissaire à la protection de la vie privée avec le consentement d'une personne qui voulait accéder à des notes d'entrevue pour prendre connaissance de ses renseignements personnels. Un enquêteur embauché par la Commission pour faire une enquête interne sur la divulgation répétée aux médias avait interviewé plusieurs employés et garanti la confidentialité des informations recueillies.

Renvoi à la Cour fédérale par le Commissaire à la vie privée du Canada et le Procureur général du Canada

Dans notre rapport annuel de l'an dernier, nous faisions état de notre intention de demander l'avis de la Cour concernant le caractère légal du couplage, par le gouvernement, des fiches de déclaration de douane des voyageurs rentrant au Canada et de la base de données de l'assurance-emploi. La cause a maintenant été déposée.

Deux questions seront posées à la Cour. La première vise à savoir si les dispositions de la *Loi sur les douanes* priment sur l'obligation faite au gouvernement, aux termes de la *Loi sur la vie privée*, d'utiliser les renseignements personnels seulement dans le but pour lequel ils sont recueillis, sauf si la personne concernée y consent. La seconde question vise à savoir si les recherches menées à l'égard des voyageurs rentrant au pays sur simple soupçon de fraude de l'assurance-emploi enfreignent la disposition visant la « protection contre les fouilles, les perquisitions ou les saisies abusives » de la *Charte canadienne des droits et libertés*.

Le Commissariat avait accepté un projet pilote pour permettre à Développement des ressources humaines Canada (DRHC) de recueillir des données et de lui présenter une proposition officielle de couplage des données (comme l'exigent les lignes directrices du Conseil du Trésor). Lorsque DRHC a entrepris de réaliser le projet avant que le Commissaire n'en ait achevé l'examen (et sans mettre en oeuvre les mesures de protection qu'il avait suggérées), le Commissaire a sollicité un avis juridique.

La Cour sera priée d'examiner le rapport entre la *Loi sur les douanes* et la *Loi sur la vie privée* par voie d'exposé de cause (un énoncé conjoint des faits par le commissaire à la vie privée et le gouvernement) aux termes du paragraphe 17(3) de la *Loi sur la Cour fédérale*. On s'attend à ce que la question de savoir si le couplage enfreint la Charte soit débattue lors de l'appel de la cause d'un plaignant à un juge-arbitre aux termes de la *Loi sur l'assurance-emploi*.

L'examen de la question par la Cour devrait avoir lieu à l'automne.

Partage des noms des requérants à la Sécurité de la vieillesse de l'Ontario et des prestataires du Régime de pensions du Québec

Un couplage un peu similaire permettrait au ministère des Ressources humaines Canada et au Régime de pensions du Canada de coupler les renseignements de prestataires du Régime de pensions du Québec et les personnes demandant la sécurité de la vieillesse, le supplément de revenu garanti et la prestation au conjoint. Puisque ces programmes fédéraux sont liés au revenu, le fait d'omettre de déclarer des revenus provenant du Régime de pension du Québec pourrait amener certains requérants à se voir verser plus que les sommes auxquelles ils ont droit.

Un projet pilote mené par le ministère des Ressources humaines Canada en 1994 et en 1996 grâce à l'utilisation de la banque de données du Régime de pensions du Canada a permis de constater que des versements excédentaires considérables de prestations fédérales étaient effectués à des personnes qui avaient mal déclaré ou qui n'avaient pas déclaré leur revenu provenant du Régime de pensions du Canada. Le ministère des Ressources humaines Canada n'a pas de raison de croire qu'il en serait autrement au Québec, mais comme il n'a pas accès aux données du Régime de pensions du Québec, il n'est pas en mesure de le vérifier.

À la fin de l'année sur laquelle porte notre rapport, ce couplage était encore à l'étude.

Le Commissariat a conclu que l'entente du ministère des Ressources humaines Canada avec l'Alberta est autorisée par la Loi sur le régime de pension du Canada et peut être considérée conforme à la collecte originale des renseignements en vertu de la Loi sur la protection des renseignements personnels. Cependant, si on désire étendre le couplage à d'autres provinces, deux autres mesures devront être prises. En premier lieu, le ministère des Ressources humaines Canada devra avertir le Conseil du Trésor du nouveau couplage en l'inscrivant dans les descriptions de ses fichiers de renseignements d'Info Source. En deuxième lieu, il devra avertir les requérants aux prestations d'invalidité du Régime de pensions du Canada que les programmes provinciaux d'assistance au revenu seront informés de l'état d'invalidité et des prestations versées.

La Sécurité de la vieillesse avisée du décès de prestataires

Un autre couplage proposé mettrait la banque de données du Régime de pensions du Québec pour identifier les prestataires du programme fédéral de la Sécurité de la vieillesse qui sont décédés. Les organismes de statistiques vitales du Québec font part des décès au programme de Sécurité du revenu du ministère des Ressources humaines Canada, mais les renseignements ne sont pas transmis dans une forme standard et souvent ne comprennent pas le NAS. Il peut alors être difficile pour le Régime de pensions du Canada d'identifier la bonne personne.

Dans les autres provinces canadiennes, les résidents contribuent au régime de pension du Canada et un avis de décès est envoyé à la Sécurité de la vieillesse ou au programme de Régime de pensions du Canada, qui le transmet à l'autre. Même si le Québec administre son propre régime, les héritiers et administrateurs des successions peuvent presumer qu'il suffit d'avertir le Régime de pensions du Québec pour que le programme fédéral le soit également. Ce n'est pas le cas. Le ministère des Ressources humaines Canada a de nombreux exemples de cas où des chèques continuent d'être versés après le décès des prestataires.

Ce couplage n'a pas encore eu lieu. Le ministère des Ressources humaines Canada finalise l'entente de partage des données avec la Régie des rentes du Québec qui administre le Régime de pensions du Québec.

d'invalidité du Régime de pensions du Canada. Ce couplage devrait permettre à la province d'économiser, mais pas au Régime des pensions du Canada.

L'Alberta remet une liste des prestataires de son régime (élément du régime de compensation) au ministère des Ressources humaines du Canada qui, à son tour, jumelle les noms y apparaissant aux données du fichier d'invalidité du Régime de pensions du Canada pour créer une liste des prestataires dont les noms figurent dans les deux fichiers et la remettre au gouvernement de l'Alberta.

Certaines personnes reçoivent de façon légitime des prestations des deux programmes, mais plusieurs verront leurs prestations diminuées ou supprimées. Les seules qui recevront une pension d'invalidité du Régime de pensions du Canada sont celles qui sont atteintes d'une invalidité prolongée. Entre-temps, l'Alberta peut verser la prestation d'invalidité provinciale. Une fois que les versements du Régime de pension du Canada débutent, les prestations provinciales peuvent être ajustées ou supprimées. L'Alberta pourra récupérer les versements en trop et réduire les coûts de son programme.

Le ministère des Ressources humaines Canada a soutenu que le jumelage des deux programmes d'assistance et de remplacement du revenu -le programme fédéral et le programme albertain- est une utilisation conforme des renseignements d'invalidité du Régime de pensions du Canada. Le Commissariat reconnaît comme une utilisation conforme des renseignements l'utilisation des renseignements d'une personne recevant des prestations pour remplacement de revenu pour déterminer son admissibilité ainsi que le montant prestations parallèles.

Afin d'uniformiser l'approche des deux organismes, notre bureau a discuté du couplage avec le bureau du Commissaire à l'information et à la vie privée de l'Alberta. Ce dernier a étudié la question et décidé de ne pas intervenir. Toutefois, si le couplage devait se faire régulièrement, le Commissaire de l'Alberta demandera qu'on précise clairement aux intéressés sur le formulaire provincial de demande de prestations que les renseignements seront partagés avec la Sécurité du revenu du Régime de pensions du Canada.

n'aurait pas à savoir que l'employé n'a pas respecté ses engagements car c'est là une question qui n'intéresse que l'employé et le Programme de prêts étudiants.

Le ministère des Ressources humaines du Canada a déclaré qu'il contacterait un seul employé du ministère pour lequel travaille le contributeur, soit la personne responsable de la liste de paye. Les agents de recouvrement tenteraient d'obtenir l'adresse et le numéro de téléphone de l'employé à la maison afin de communiquer avec celui-ci à son domicile. Si le contributeur et le ministère pouvaient s'entendre sur le paiement de la dette, l'employeur n'aurait pas à intervenir davantage. Au cas où une saisie serait nécessaire, des dispositions seraient prises avec le bureau de la paye et non avec les surveillants de l'employé.

Le Programme de prestation d'invalidité de l'Alberta et les Prestations d'invalidité du régime de pension du Canada

Ce couplage vise à comparer la liste des personnes recevant des prestations d'invalidité du Régime de pensions du Canada à la liste des prestataires du Programme de prestations d'invalidité de l'Alberta. Il se limite actuellement à l'Alberta, mais le ministère des Ressources humaines Canada prévoit signer des arrangements similaires avec d'autres provinces et territoires.

Cette initiative, mise en veilleuse depuis deux ans, veut en partie répondre à une question soulevée par le Vérificateur général dans son rapport de 1996, où on faisait mention d'une étude de Statistique Canada qui établissait à 17 pour cent le taux des personnes admissibles aux prestations d'invalidité du Régime de pensions du Canada qui touchaient également des prestations de la Commission d'invalidité. Le Vérificateur général estimait que la somme de 42 millions de dollars pourrait être économisée annuellement par l'élimination de paiements en double. Curieusement, cet énoncé ne tient pas compte du fait que le Régime de pensions du Canada est le premier à verser des prestations avant le régime provincial. Les prestations obtenues de la province n'affectent habituellement pas le droit à recevoir les prestations

L'année dernière il y a eu peu d'activités de couplage de données, sauf à l'égard des Ressources humaines Canada. Alors que d'autres institutions étaient plutôt sur le terrain et posaient des questions générales sur l'ensemble du processus, les ministères, une fois que la procédure d'approbation globale leur est expliquée (évaluations détaillées, étude de faisabilité et soumission du projet au Commissaire à la protection de la vie privée), prennent conscience de toute la complexité de la question. À l'occasion, les demandes de renseignements sur le couplage des données révèlent plus un besoin de comprendre ce qu'est le couplage de données que l'intention d'en exécuter un.

Les contrevenants au Programme canadien de prêts aux étudiants et le fichier des employés gouvernementaux

Ce couplage, décrit pour la première fois dans notre dernier rapport annuel, vise à comparer la liste des contrevenants au Programme canadien de prêts aux étudiants à la liste de paye des employés fédéraux. Ce faisant, DRHC serait en mesure d'identifier les employés qui ont contrevenu aux ententes de remboursement de leur prêt et ainsi récupérer ce qui est dû de parties intéressées qui ne pourraient pas s'y opposer.

La Loi sur la protection des renseignements personnels autorise les communications de données personnelles afin de retracer quelqu'un ayant une dette envers une société de la Couronne ou encore à qui une société de la Couronne doit de l'argent. Cela diffère des listes de couplages utilisées pour déterminer qui *pourrait* bien avoir une dette, comme dans le cas du couplage des déclarations de douanes des voyageurs aux listes de prestataires d'assurance-emploi. La distinction est importante.

Une fois que le programme de prêts aux étudiants aurait permis d'établir une liste de contrevenants et que cette liste aurait été comparée à la liste de paye du gouvernement, le Commissaire a voulu s'assurer que le remboursement des dettes ne nuirait pas à l'employé à son travail. À moins qu'une saisie de salaire soit nécessaire, l'employeur

début des prestations, le montant hebdomadaire, l'état et le type de demande, la période d'attente et l'occupation antérieure. Quoique DRHC peut aussi communiquer d'autres renseignements à des fins d'enquête sur demande écrite, l'administration centrale doit autoriser cette communication. Toute divulgation au MEEST exige le consentement de la personne concernée.

Le personnel de Citoyenneté et Emploi a expédié un avis à ses collègues de la C.-B. leur rappelant de communiquer à DRHC seulement les données personnelles prévues en vertu du protocole d'entente de 1997. Celui-ci établit clairement quels renseignements peuvent être communiqués, de quelle façon et à quel moment, et supprime tout formulaire de consentement signé. Le personnel du Commissariat enquête actuellement sur plusieurs plaintes en bonne et due forme visant Revenu Canada.

Il semble que la collecte proposée aurait été traitée par M. David Flaherty, Commissaire à l'information et à la vie privée de la Colombie-Britannique, qui a examiné la loi et les ententes de partage proposées. Quoique inquiet, il a conclu que le ministère pouvait légalement communiquer avec tout organisme susceptible de vérifier l'éligibilité aux prestations. M. Flaherty est à l'origine de la transparence du formulaire et du consentement détaillés.

Dans un énoncé public en date du 27 janvier, M. Flaherty a souligné que même si la collecte de renseignements est bel et bien sanctionnée par la loi, son impact n'en a pas moins des effets néfastes au chapitre de la vie privée des prestataires. Il ajoute toutefois que l'étendue de ses pouvoirs est limitée du fait qu'une loi ou un règlement peut supplanter le droit à la vie privée lorsqu'il est établi qu'il va de l'intérêt public.

Plusieurs groupes qui font front commun dans la lutte contre la pauvreté ont depuis entrepris des poursuites juridiques contre ce type de collecte. Face à la controverse, DRHC a revu son formulaire de consentement, qui fait maintenant partie intégrante du formulaire de demande, et émis un feuillet informatif ainsi qu'une série de questions et de réponses sur le processus des prestations à l'intention des demandeurs.

Bien sûr, le partage des renseignements ne se limite pas au gouvernement fédéral. En fait, des échanges ont souvent lieu entre divers paliers gouvernementaux (fédéral, provincial et municipal) et parfois même entre pays. La *Loi sur la protection des renseignements personnels* autorise le partage en vertu d'ententes pour l'administration ou l'application d'une loi ou encore pour mener une enquête autorisée par la loi. Ces ententes ne nécessitent pas le consentement des personnes et même si le gouvernement est tenu d'avertir le public, l'avis paraît habituellement dans *Info Source* seulement.

Des avis précis peuvent avoir des conséquences intéressantes. Ainsi, examinons le cas d'une entente provinciale de partage en Colombie-Britannique qui, une fois expliquée au public, a suscité toute une salve de critiques. Lorsqu'une nouvelle loi est entrée en vigueur en avril 1997, les ministères des Ressources humaines et celui de l'*Education Skills and Training* (MEST) de la province ont communiqué avec les prestataires d'aide au revenu, jeunes au travail et les prestataires d'invalidité pour les avertir qu'ils devaient consentir à ce que les ministères recueillent des renseignements à leur sujet détenus par diverses autres organismes. Le paragraphe principal se lisait comme suit:

J'autorise toute personne qui détient des renseignements ou des documents pertinents à les communiquer sur demande verbale ou écrite aux employés du ministère des ressources humaines ou MEST. Je comprends que ces renseignements ou documents peuvent provenir, sans s'y limiter, de: Ressources humaines Canada, la Commission des accidents du travail, la *Insurance Corporation of British Columbia*, le programme d'aide aux étudiants de la Colombie-Britannique, la Direction des véhicules automobiles, la *British Columbia Assessment Authority*, le *Registrar of Companies*, Titres de biens-fonds, la *Lottery Corporation of British Columbia*, les Statistiques de l'état civil, la Sécurité de la vieillesse, le Régime de pension du Canada, des ministères fédéraux, provinciaux ou municipaux, Citoyenneté et Immigration Canada, la police, les organismes fédéraux ou d'Etat d'aide des Etats-Unis d'Amérique ou de tout autre pays, Equifax, toute institution financière, caisse populaire, service

Les ententes de partage gagnent en visibilité

Il semble que jusqu'en 1996 la liste était compilée annuellement afin de placer les nouveaux employés aux échelons salariaux appropriés selon leur expérience et leurs qualifications et en fonction de la gamme d'autres employés effectuant les mêmes tâches. Les cadres supérieurs utilisaient eux aussi la liste durant les évaluations de rendement annuelles pour uniformiser la démarche d'évaluation à la Commission. Les seules personnes qui y avaient accès étaient deux cadres supérieurs et leurs secrétaires, la personne qui compilait la liste et une personne qui l'analysait pour préparer des rapports destinés aux cadres supérieurs, de même qu'au directeur général du personnel.

La Commission a confirmé que la liste détenue par le député et le *Canadian Farm Enterprises Network* est bien une copie de l'original. En raison du débat politique intense qui a lieu dans l'Ouest canadien au sujet du mandat et des salaires du personnel de la Commission, il s'agit probablement là d'un cas classique de fuite de renseignements passés anonymement.

La Commission a embauché une entreprise privée pour enquêter sur la fuite et tiendra le Commissariat au courant des progrès accomplis; elle lui fournira une copie du rapport d'enquête. Quoiqu'il ait convenu d'attendre les résultats de l'enquête en cours, le Commissaire à la protection de la vie privée du Canada se réserve le droit de mener sa propre enquête.

Pratiquement toutes les lois traitant de vie privée comportent des dispositions autorisant les gouvernements à partager les renseignements pour administrer ou faire appliquer divers programmes d'aide. Quoiqu'on puisse comprendre certains partages, on remarque maintenant que ceux-ci prolifèrent. À moins d'être un lecteur régulier de la *Gazette du Canada* ou d'autres publications gouvernementales, le public n'est pas au courant de la plupart des couplages. *Info Source*, le répertoire qui contient la description de tous les fichiers de renseignements personnels détenus par le gouvernement fédéral, décrit le partage des renseignements en termes très généraux.

Après que des listes aient été transmises au gouvernement du Nouveau-Brunswick et à la municipalité de Winnipeg, plusieurs électeurs ont communiqué avec Elections Canada pour demander que leurs noms n'y figurent plus. Parce qu'il était trop tard pour retirer les noms de la liste fédérale, Elections Canada a demandé à ce gouvernement et à cette municipalité de retirer ces noms des listes locales si la liste fédérale constituait leur unique source d'information.

Puisqu'en soi il s'agissait là d'une divulgation de renseignements personnels, mais consentie par des personnes qui se prévalaient de leur droit, Elections Canada a fait savoir que la description de sa base de données dans *Info Source* serait modifiée afin de clairement indiquer les cas de divulgations possibles.

Elections Canada a assuré le Commissaire que toutes les futures ententes comporteraient des dispositions précises exigeant que tous les autres paliers gouvernementaux satisfassent à ces demandes de retrait de nom (il est à remarquer que les ententes en vigueur seront également modifiées).

Dans un autre ordre d'idées, l'obtention du consentement des contributeurs pour la mise à jour de la liste électorale à partir de leur déclaration sur le revenu semble avoir réussi. En effet, malgré une certaine anxiété au tout début, environ 81 pour cent des contribuables ont accepté ce transfert, ce qui indique que la notion de consentement éclairé fonctionne.

Incidents

Au début de mars dernier, la Commission canadienne du blé a averti le Commissariat qu'un député et le *Canadian Farm Enterprises Network* avaient communiqué aux médias la liste des salaires exacts de tout le personnel et des membres de la Commission. On retrouvait sur celle-ci les noms des employés, des gestionnaires ainsi que les personnes nommées par le gouverneur général en conseil, soit environ 400 personnes. Quoique la *Loi sur la protection des renseignements personnels* autorise la communication de certains renseignements au sujet d'employés – exemptant ces renseignements de la définition de renseignements personnels dans l'intérêt public pour une plus grande responsabilisation –, les salaires exacts sont protégés.

inscrit, et a refusé pour la quatrième fois sa demande d'ordonner aux compagnies de téléphone de fournir à leurs abonnés non inscrits le service de blocage permanent de l'affichage de leurs coordonnées. Ce nouveau refus oblige les abonnés non inscrits à continuer de composer *67 (appareils à tonalité) ou 1167 (appareils à cadran) avant chaque appel.

Cette dernière ordonnance du CRTC, bien qu'impartiale, vient cependant renforcer notre droit à la vie privée puisque la baisse des tarifs mensuels permettra à plus d'abonnés de se procurer un numéro non inscrit. Mais ne baissons pas les bras : il nous reste encore des efforts à faire. Chaque abonné doit lire attentivement le début de son annuaire, aux pages expliquant les services spéciaux offerts par sa compagnie de téléphone et les façons que cette dernière lui offre de protéger sa vie privée. Trop peu de gens prennent le temps de lire ces pages afin d'ap-prendre comment retirer leurs noms des annuaires imprimés, des afficheurs, des annuaires électroniques publiés sur l'Internet (tel Canada 411), et des listes vendues aux compagnies de marketing direct.

Dix minutes de lecture pourraient nous éviter bien des désagréments, allant du simple coup de fil d'une compagnie de nettoyage de tapis à l'heure du repas en passant par le déluge de publicités dans notre boîte aux lettres.

Liste électorale permanente

Les gestionnaires d'Élections Canada continuent de tenir le Commissariat informé de l'administration de la liste électorale permanente. Créée pour la tenue de la dernière élection fédérale, cette liste peut être mise à jour avec le consentement des électeurs à partir des fichiers de données provenant de l'Immigration et du Revenu, ainsi que de diverses sources provinciales.

La *Loi électorale du Canada* autorise Elections Canada à signer avec les provinces et les municipalités des ententes qui permettent à ces dernières d'utiliser les listes d'électeurs de la région qui y consentent pour dresser des listes pour les élections locales. Ces listes (moins les noms de ceux qui ont refusé d'y figurer) ont déjà été transmises à plusieurs provinces et municipalités dans le cadre d'ententes signées avec Elections Canada.

Annuaire téléphonique : fin de la saga

Comme l'expliquaient les derniers rapports annuels du Commissaire à la protection de la vie privée du Canada, les renseignements personnels que les compagnies de téléphone publient sur leurs abonnés dans leurs annuaires valent leur pesant d'or. Mais les abonnés viennent heureusement de récupérer un certain contrôle sur ces renseignements.

Il y a quatre ans, l'éditeur indépendant White Directories of Canada Inc. demandait accès aux bases de données des compagnies de téléphone pour pouvoir publier ses propres annuaires. Le Conseil de la radiodiffusion et des télécommunications (CRTC) s'était dit d'accord, à condition que chaque abonné ait la possibilité de refuser que ses renseignements soient communiqués à des éditeurs indépendants. La White Directories avait interjeté appel de cette décision auprès du Gouverneur en Conseil, car ses annuaires auraient été moins complets que ceux des compagnies de téléphone. Le Gouverneur en Conseil avait donné raison à la White Directories, mais avait ordonné au CRTC de se pencher sur la protection, au sens large, des renseignements personnels d'abonnés.

En décembre 1996, le CRTC remettait son rapport au Gouverneur en Conseil, dans lequel il reconnaissait l'existence de certains problèmes en matière de protection des renseignements d'abonnés, et annonçait son intention de tenir des audiences publiques sur la non-inscription aux annuaires. Ces audiences ont eu lieu à l'automne dernier et le Commissaire y a proposé entre autres que le CRTC revoie le montant mensuel de cinq dollars imposé qui était un obstacle dans certaines provinces pour certains abonnés qui autrement auraient choisis de ne pas figurer dans les annuaires.

En février dernier, le CRTC a émis son Ordonnance 98-109, dans laquelle il a imposé à toutes les compagnies de téléphone un plafond mensuel de deux dollars par numéro non inscrit, ainsi qu'une obligation de permettre aux abonnés de régler tout frais de changement de numéro par versements. Le CRTC ne s'est cependant pas rendu aux arguments du Commissaire en faveur de la gratuité d'un numéro non

institutions financières se sont implantées dans un autre domaine, soit le traitement des données des autres compagnies.

Plusieurs audiences du Comité et rapports qui lui ont été présentés ont mené à élaborer des règlements exigeant que les institutions financières établissent des procédures régissant la collecte, la conservation, l'utilisation et la communication des renseignements des clients, informant ces derniers des procédures, nomment un agent à l'interne chargé de recevoir les plaintes et fassent rapport annuellement sur les plaintes; l'industrie avait déjà adopté toutes ces mesures. L'Association des banquiers canadiens a mis en oeuvre le code modèle de l'Association canadienne de normalisation et nommé un ombudsman pour son secteur.

On peut considérer tout cela comme un progrès, mais il manque deux éléments essentiels : les droits de poursuite et un mécanisme indépendant de révision. Une institution financière n'est pas tenue de se soumettre à l'arbitrage ou à une vérification. Sans ces derniers, la protection des renseignements personnels n'est qu'une illusion. Bref, c'est peu de résultats pour six années de travail.

L'espoir d'une protection efficace de la vie privée dans les institutions financières repose maintenant sur une loi qui autoriserait le gouvernement fédéral à réglementer le secteur privé, promise pour l'an 2000. (Voir la page 12).

Après plusieurs rencontres et à la veille de la comparution du Commissaire devant le Comité des finances à cet égard, DRHC a négocié plusieurs modifications, entre autres que les personnes conservent tous leurs droits en vertu de la *Loi sur la protection des renseignements personnels*. Ainsi, les couplages avec les institutions fédérales se limitent à ceux qui sont nécessaires pour administrer la *Loi sur le Régime de pensions du Canada*, on ne fera plus renvoi aux activités provinciales citées comme légitimes à des fins de communications, et on inclura des renvois spécifiques lorsqu'il s'agit de programmes qui ne relèvent pas de DRHC mais dont l'administration exige des données du Régime de pensions du Canada. Des changements similaires ont été apportés à la *Loi sur la sécurité de la vieillesse*.

Comme dans toute négociation, il y a eu des compromis acceptables. Le Commissaire apprécie le fait que le personnel de DRHC a fait preuve de sensibilité à l'égard du respect de la vie privée de sa clientèle et de détermination à rédiger une loi convenable.

Groupe de travail sur l'avenir des institutions financières

Le groupe de travail a été créé afin d'examiner la structure et les questions de principe entourant les institutions financières et les fournisseurs non traditionnels de services financiers. On s'attend à ce que le rapport soit déposé en septembre 1998.

Le premier mémoire que le Commissaire a déposé au Parlement sur la protection du caractère confidentiel des renseignements personnels de clients remonte à 1992 lorsqu'une nouvelle loi a changé tout le régime de réglementation des institutions financières. Le rapport traitait des menaces que posaient à la vie privée les nouveaux services financiers de propriété commune, qui font appel, entre autres, au partage des renseignements personnels des clients ainsi que les moyens technologiques dont disposent ces institutions pour recueillir et assimiler les données personnelles et établir le profil de leurs clients.

Dans ce rapport au Parlement ainsi que dans des mémoires ultérieurs, le Commissaire a recommandé que le gouvernement prenne des règlements pour protéger les données des clients. Entre-temps, les

Au nombre des nombreuses modifications apportées à la *Loi sur le régime de pensions du Canada*, nous notons que plusieurs renseignements contenus dans les dossiers de pension. En tentant d'assouplir la protection l'accès et à la communication des renseignements personnels contenus rigoureuse que le Régime de pensions du Canada et la *Loi sur la sécurité de la vieillesse* confèrent à ces renseignements (ce qui, d'après l'Développement Ressources humaines Canada, nuisait à ses opérations internes), on proposait d'accorder un pouvoir discrétionnaire considérablement élargi au ministre et de beaucoup accroître la collecte, les utilisations et les communications admissibles.

Le projet de loi contenait également une sorte de loi sur la protection des renseignements personnels tronquée et imparfaite qui semblait esquiver les droits d'accès des personnes et ne prévoyait pas d'avis au Commissaire pour les communications faites dans l'intérêt public.

La grande faille dans cette approche est que les articles concernant la communication des renseignements personnels dans les autres lois du Parlement prennent sur les limites particulières contenues dans la *Loi sur la protection des renseignements personnels*. Bref, en tentant d'assouplir sa propre loi habilitante, le ministre risque d'évider la *Loi sur la protection des renseignements personnels*. Le Commissaire a reconnu que cela n'était peut-être pas voulu, mais c'est ce qui se produisait néanmoins. Il a recommandé à DRHC que toutes les utilisations et les communications soient conformes au but original de la collecte plutôt qu'une approbation générale permettant au ministre de communiquer des renseignements personnels aux fins administratives d'une autre loi fédérale, d'une loi provinciale ou d'une activité. Il a suggéré que le ministre envisage d'adopter l'approche prise dans la *Loi sur l'impôt sur le revenu* qui autorise des communications limitées et précises.

Le projet de loi autorisait aussi le ministre à recueillir des renseignements du gouvernement fédéral, des gouvernements provinciaux, de leurs organismes publics et des renseignements pertinents à sans tenter de limiter la collecte à des renseignements pertinents à l'administration du Régime de pensions du Canada ou même à quelque programme que ce soit de DRHC.

arbitres ou quiconque assiste le CCRT. Même si les commissions et agences peuvent trouver difficile de fonctionner en vertu des dispositions de transparence de ces lois, leur fonction est de protéger les Canadiens et non les bureaucrates et les personnes nommées. Le Commissaire a incité le Conseil à ne pas laisser les personnes ou les institutions formuler leurs propres petites dérogations et exemptions à des lois comme la *Loi sur la protection des renseignements personnels*.

Le fait que cette même question soit devant les tribunaux mérite encore davantage d'attention. Un homme s'était plaint au Commissaire qu'on lui avait refusé l'accès à ses renseignements personnels contenus dans les notes d'un membre du CCRT qui avait entendu sa cause. Le CCRT a plaidé que les notes prises par un membre ne tombent pas sous le contrôle du CCRT. Le Commissaire a jugé que la plainte était fondée et il a porté le refus d'accès du CCRT devant la Cour. Il a demandé instamment au Comité parlementaire d'attendre le jugement de la cour avant d'adopter cette modification.

Au moment où nous allions sous presse, le projet de loi avait reçu la sanction royale. En vertu de cette loi, le Conseil peut maintenant ordonner aux employeurs de communiquer aux syndicats les noms et adresses des travailleurs à domicile. L'ordonnance doit stipuler la façon de communiquer, les moments et les périodes au cours desquels les communications sont permises, de même que les conditions nécessaires pour protéger la vie privée des travailleurs à domicile. Si on juge que la vie privée et la sécurité des employés ne peuvent être assurées autrement, le consentement des employés pourrait être demandé. Ce faisant, on reconnaît que la vie privée est en jeu mais on contourne la difficulté en permettant au Conseil de s'en remettre à la décision de l'employé.

À l'encontre de la recommandation émise, le Parlement a choisi de ne pas attendre le jugement de la Cour sur la question de l'accès aux notes prises par les membres. Non seulement ces notes peuvent-elles être consultées seulement avec le consentement du membre, mais l'exemption s'applique à toutes les personnes nommées à la résolution des plaintes ou des litiges.

Code canadien du travail (projet de loi C-19)

Cette loi régit les relations de travail dans les industries sous réglementation fédérale telles les banques, les télécommunications et le transport. Le Commissaire a exprimé des réserves au sujet des modifications qu'on retrouvait dans le projet de loi 66 du Parlement antérieur. Avec la tenue des élections en 1997, le projet est mort au Feuilleton.

Une version légèrement modifiée du projet de loi (l'actuel C-19) a été déposée en novembre 1997. Lors de sa comparution devant le comité parlementaire, le Commissaire a souligné deux articles préoccupants. L'article 50 prévoit que les syndicats pourront communiquer avec les travailleurs à domicile. Puisque cela exige des employeurs et, à l'occasion, du Conseil canadien des relations de travail (CCRT) de faire connaître le lieu de travail des travailleurs à domicile, cela équivaut à divulguer leur adresse domiciliaire.

Souignant que la plupart des personnes ont une attente élevée de respect de leur vie privée à leur domicile, le Commissaire a proposé que la loi exige que le travailleur à domicile donne son consentement pour la communication de son adresse domiciliaire plutôt que d'exercer une option de refus. L'affiliation syndicale n'est pas obligatoire, et les syndicats pourraient faire du démarchage auprès des travailleurs à domicile à l'adresse de travail de l'employeur. Par exemple, la *Loi sur les relations de travail dans la fonction publique* stipule que les organismes fédéraux doivent donner aux nouveaux employés une carte d'entregistrement syndical qu'ils peuvent remplir et retourner s'ils le désirent. Les adresses domiciliaires ne sont pas communiquées aux syndicats de la fonction publique.

Le deuxième article (54) empêche essentiellement les personnes d'accéder à leurs renseignements personnels contenus dans les notes prises par les personnes nommées au CCRT ou le ministre sans le consentement des personnes nommées. Cette mesure spéciale semble soustraire à l'application de la *Loi sur la protection des renseignements personnels* et de la *Loi sur l'accès à l'information* les membres du CCRT, les

faux serment, etc.). L'ADN serait alors prélevé de la plupart des suspects (puisque la plupart des infractions au Code criminel sont criminelles), de façon presque aussi automatique que les empreintes digitales.

Le ministre de la Justice s'est fortement prononcé contre cette tentative d'étendre la portée du dépistage génétique de suspects en invoquant des motifs constitutionnels. Le Commissariat s'oppose au dépistage élargi parce que cela constitue une utilisation excessive et inutile des pouvoirs d'intrusion de l'Etat, qui devraient être mis en oeuvre seulement dans des situations étroitement contrôlées et après l'obtention d'un mandat d'un juge à cet effet.

Le projet de loi n'était plus au Feuilleton au moment d'aller sous presse.

Des documents de position sur ces questions – la collecte obligatoire d'échantillons d'ADN de suspects dans le cadre d'un crime particulier et l'établissement d'une banque de données – peuvent être obtenus de notre bureau ou consultés sur notre site Internet.

L'ADN et le système judiciaire criminel

Le rapport annuel de l'an dernier traitait du projet de loi sur l'ADN qui venait d'être déposé devant la Chambre des communes. La Loi sur l'identification par les empreintes génétiques tentait d'établir une banque de données génétiques à partir de prélèvements sur des condamnés afin d'aider la police à identifier les auteurs de crimes non résolus. Le projet de loi constituait la deuxième phase du plan du gouvernement pour réglementer l'analyse génétique comme outil d'identification des auteurs de crimes à partir de traces d'ADN laissées sur les lieux du crime. La première phase de la loi permettant aux forces policières d'obtenir un mandat pour l'obtention d'échantillons génétiques de suspects a été adoptée en 1995.

Avec la tenue de l'élection fédérale en avril 1997, le projet de loi est mort au Feuilleton. En septembre 1997, le gouvernement a déposé un projet de loi très similaire, le projet de loi C-3, qui suscitait des inquiétudes sous plusieurs aspects. Lors de sa comparution devant le Comité permanent sur la justice et les droits de la personne en mars 1998, le Commissaire a fait plusieurs recommandations, dont :

- prélever un échantillon d'ADN d'un condamné pour crimes violents seulement lorsqu'il y a risque de récidive et qu'on est presque sûr de trouver, sur les lieux du crime, des substances génétiques;
- détruire l'échantillon après obtention de l'information aux fins d'identification; seule l'analyse serait conservée dans le dossier de police;
- s'assurer que l'échantillon et l'analyse offerts spontanément par les personnes pour aider la police sont détruits immédiatement et ne sont pas utilisés pour faire quantité d'enquêtes sur d'autres types de crimes.

Nous sommes inquiets des pressions qu'exercent certains groupes et politiciens pour le prélèvement automatique d'échantillons génétiques de toute personne accusée d'un acte criminel, ce qui pourrait compromettre un acte relativement bénin ou un acte non violent (prêter un

ligne qui se tiendra avec d'autres étudiants à travers le pays en vue de négocier une entente intergouvernementale sur les droits à la vie privée sur Internet. L'entente sera par la suite soumise pour ratification aux écoles participantes.

Le Cabinet juridique offre de la documentation éducationnelle de haut calibre aux enseignants et aux étudiants sur la justice et les questions des droits de la personne. Quoique conçu à l'intention des étudiants du niveau secondaire, le site mérite que quiconque s'interroge sur la technologie y fasse une halte afin de voir comment la technologie affecte notre vie et de savoir comment équilibrer progrès technologiques et valeurs humaines comme la vie privée.

Des liens à ces deux sites existent à partir de notre site.

Industrie Canada s'engage virtuellement à l'égard de la vie privée

Le Groupe de travail d'Industrie Canada sur le commerce électronique a mis sur pied un site Web qui explique l'importance de la vie privée dans la conduite des transactions électroniques et offre une trousse de travail pour aider les personnes à protéger leurs renseignements personnels.

La trousse contient des liens menant vers l'éducation des consommateurs, les codes de pratiques, le cadre législatif et les technologies d'appui à la vie privée ainsi qu'un document de travail sur une loi applicable au secteur privé, intitulé *La protection des renseignements personnels - Pour une économie et une société de l'information au Canada*. Vous pouvez joindre ce site à partir de notre site Internet.

En attente du projet « Défectives privés »

À la mi-mai, ce groupe a publié un jeu interactif sur disque compact intitulé *Jouer sans se faire jouer : la première aventure des trois petits cochons dans le cyberspace*. Le jeu met en vedette trois cochonnets et un gros méchant loup de la cyberspace en vue d'enseigner aux enfants à discerner les techniques de publicité électronique envahissantes et trompeuses et l'importance de ne pas divulguer de renseignements personnels sollicités électroniquement.

Le site Web du groupe Réseau Education mérite bien une visite en raison de sa vaste collection de documents éducationnels électroniques en ligne sur la vie privée.

Les étudiants du secondaire ne sont pas en reste. À compter de septembre 1998, ils pourront participer au Projet « Défectives privées » mis sur pied en vue de fêter le cinquantième anniversaire de la signature de la Déclaration universelle des droits de l'homme des Nations Unies qui reconnaît l'importance de la vie privée au nombre des droits de la personne.

Ce projet est issu du Centre de recherche et d'enseignement sur les droits de la personne de l'Université d'Ottawa, avec l'appui généreux de la Banque Royale du Canada, de Patrimoine Canada, de l'honorable députée et présidente du Comité permanent des droits de la personne et de la condition des personnes handicapées, Mme Sheila Finestone, ainsi que de notre bureau. Le Cabinet juridique est une composante du Rescol canadien et offre aux visiteurs l'occasion d'essayer plusieurs scénarios possibles et tirer leurs propres conclusions sur l'importance de protéger les renseignements personnels. En prime, le projet offre de l'information pratique sur le processus de législatif de comités parlementaires et des négociations intergouvernementales.

Cet automne, les étudiants pourront mettre en pratique ces informations puisqu'on invite les écoles à tenir leurs propres audiences parlementaires sur les droits à la vie privée au siècle à venir et à publier leurs conclusions dans le cabinet juridique. La prochaine étape et une qui rapprochera vraiment les personnes sera le forum de discussion en

montrent particulièrement agacées par les sollicitations téléphoniques, le publipostage, le pistage de leurs données et les échanges et ventes courantes de leurs renseignements personnels.

Les répondants reconnaissent certes l'existence de lois gouvernementales sur la vie privée, mais le fait que le gouvernement soit, lui aussi, susceptible d'abuser des renseignements personnels les inquiète. Les personnes interrogées se prononcent énergiquement en faveur d'assurer elles-mêmes le contrôle de leurs renseignements personnels et ne veulent pas être pénalisées en cas de refus de communication

Par ailleurs, on estime que le processus pour déposer une plainte devrait être simplifié et être doté de garanties à l'effet que les contreprises respectent la loi. Enfin, pratiquement tous ont jugé qu'une formation doit être offerte dans le domaine de la vie privée.

Dans l'ensemble, le *Forum sur la vie privée* s'est révélé être pour les Canadiens un formidable outil d'information sur des questions de vie privée en plus de permettre l'évaluation de leurs réponses. Hébergé sur une partie du Réseau Éducation Médias appelée *Pages sur la vie privée*, le Forum est une mine de liens et de documentation. Plus de la moitié des 266 participants au sondage ont déclaré que le *Forum sur la vie privée* avait accru leur compréhension et surtout modifié leur façon de percevoir les questions de vie privée. C'est qu'on appelle une réussite. Qui sait combien d'autres personnes auraient participé s'il y avait eu plus de temps.

Cette initiative de la démocratie électronique a été un franc succès, surtout si l'on considère son échéancier très serré. L'effort extraordinaire de mobilisation des Canadiens à ce débat a été un des grands moments de tout l'exercice.

Terrain de jeu pour les enfants

Mieux informer les jeunes cybersurfers a été l'une des priorités du Réseau-Education depuis son lancement en 1996. Le Réseau a maintenant trouvé comment enseigner aux jeunes à protéger leur vie privée sur Internet.

Forum sur la vie privée —

expérience en démocratie électronique

Ce document de travail sur une loi applicable au secteur privé, on se le rappellera, a été rendu public le 24 janvier dernier, et la période de commentaires a pris fin le 31 mars (voir page 12). Les intéressés n'avaient donc que peu de temps à leur disposition pour faire connaître leurs vues sur le type de protection des renseignements personnels que devrait offrir le secteur privé.

Des représentants du public et des défenseurs des droits des consommateurs de partout au pays y sont parvenus. Afin de se faire entendre, ils se sont mobilisés à la vitesse de l'éclair pour monter un site Internet interactif ainsi qu'un groupe de discussion appelé *Forum sur la vie privée*. Le *Forum sur la vie privée* était le fer de lance du Réseau Éducation

Médias, du Centre pour la défense de l'intérêt public, de la Coalition canadienne de l'information publique, de l'Association canadienne des consommateurs, de la Fédération nationale des associations de consommateurs du Québec, de la Bibliothèque publique d'Ottawa et de Télécommunautés Canada.

Le site comprenait de la documentation générale sur des questions de vie privée, des liens menant à d'autres sites pertinents ainsi qu'un sondage en direct permettant aux Canadiens d'exprimer leurs opinions sur la protection des renseignements personnels. Le Forum comportait un groupe de discussion qui permettait aux personnes de traiter en temps réel de questions de vie privée.

Le but du sondage du Forum n'était pas de recueillir des données scientifiques mais plutôt de connaître l'opinion des personnes sur des énoncés explicites sur la protection des renseignements personnels. Le sondage a démontré un fort consensus sur plusieurs questions.

L'un des messages les plus clairs, que le Commissariat appuie vivement, est que les personnes interrogées sont insatisfaites des pratiques de l'information actuellement en vigueur dans le secteur privé. Elles se

vie privée dans l'environnement électronique devrait appuyer cet effort d'autoréglementation plutôt que d'attendre l'adoption d'une loi qui l'y contraindrait.

La deuxième solution est le projet *Privacy References Project* (projet P3P), qu'un consortium surveillant le développement du Web a lancé en mai 1997. Le projet P3P permet au surfeur de préciser ses préférences en matière de vie privée (par le biais de son fureteur) et aux sites Web de rendre publiques leurs pratiques de protection des renseignements personnels. Le surfeur est alors en mesure d'accéder à des sites compatibles et de se tenir loin des sites inamicaux ou de négocier avec eux. Le projet P3P est en cours de développement et ne sera opérationnel que dans plusieurs mois. Son avenir est incertain, et on ne sait pas dans quelle mesure il sera accepté par les propriétaires de sites Web.

Lorsqu'il s'agit de l'Internet, on constate avec regret qu'il est encore plus rentable de commettre des intrusions dans la vie privée que de la protéger. Jusqu'à ce que la situation change, le mot d'ordre doit être : vigilance!

Existe-t-il des solutions à toutes ces intrusions?

Ce n'est pas un constat relevant de la science-fiction. L'an dernier, on a relevé des centaines d'intrusions dans les ordinateurs les mieux protégés du monde, soit ceux du Pentagone, du FBI et de la NASA. Si vous jugez vos renseignements peu importants, repensez-y. En effet, la spécialité de certains intrus est de recueillir suffisamment de renseignements vous concernant pour usurper votre identité. L'intrus demandera, en votre nom, des cartes de crédit, louera ou achètera des biens et des services, occupera un emploi et vous laissera toutes les factures et l'impôt sur le revenu à payer, sans parler d'une réputation à refaire. Les vols d'identité de ce type sont à la hausse en raison des transactions électroniques.

À l'exception des trucs susmentionnés, il existe peu d'options pour protéger la vie privée sur l'Internet. Les lois sont peu utiles parce qu'elles varient d'un pays à l'autre et que l'Internet n'a pas de frontières. Les codes d'éthique (comme celui de 1996 de l'Association canadienne de Fournisseurs Internet) sont de belles déclarations d'intention, mais leur adoption est volontaire et ils sont inutiles s'ils sont enfreints. Pourtant, deux nouvelles solutions récentes pourraient faire une différence.

La première est le programme TRUSTe. Lancé par un groupe d'entreprises américaines et de groupes de défense en 1997, le programme cherche à créer une atmosphère de confiance pour les communications et les transactions électroniques. TRUSTe incite les sites Web à informer les surfeurs des pratiques qu'ils adoptent en matière de protection de la vie privée ainsi que de l'utilisation qu'ils comptent faire des renseignements personnels qu'ils recueillent. Un site qui souscrit à TRUSTe affiche le logo du programme sur sa page d'accueil (et peut donc faire l'objet d'une vérification de la conformité). Malheureusement, très peu de sites se sont joints au programme; en avril 1998, on comptait seulement 75 participants. Il semble que les entreprises hésitent à s'y joindre par crainte des sanctions qui pourraient être imposées en cas d'infraction. Toutefois, une entreprise qui souhaite vraiment gagner la confiance du client en protégeant sa

On ne le répètera jamais assez : le courriel sur l'Internet est à peu près aussi confidentiel et sécuritaire qu'une carte postale acheminée par la poste. Tout et chacun – du personnel de votre fournisseur Internet aux amis de vos correspondants et collègues – tous peuvent consulter votre message électronique à partir du moment où vous cliquez sur le bouton d'envoi de votre ordinateur. À moins que vous et votre correspondant ne chiffriez votre correspondance (voir *Peut-on garder un secret?* à la page 65), n'y incluez pas de renseignements de nature délicate (numéro de carte de crédit, dates de vos vacances, renseignements médicaux, etc.). Vous pouvez aussi faire expédier votre message – et parfois recevoir la réponse – par une messagerie confidentielle sans que vos renseignements personnels y soient attachés. Vous trouverez une liste de ces messageries sur notre site Internet.

Un autre type d'invasion de la vie privée associé au courriel est l'inondation. Le démarcheur de marketing direct électronique qui obtient votre adresse électronique vous inonde de publicités non sollicitées. Parce que les publimessages électroniques sont tout aussi désagréables que la publiposte, et qu'ils sont coûteux (vous demeurez en ligne pendant que vous recevez, lisez et supprimez les publimessages), la plupart des fournisseurs de services Internet ont développé des façons d'interdire l'inondation de votre boîte aux lettres. Renseignez-vous!

Le piratage

Le piratage (ou "bidouillage") est l'accès non autorisé à votre système et à vos fichiers. L'Internet, qui est un réseau mondial, est un véritable paradis pour le bidouilleur. L'accès aux dossiers de votre fournisseur de services Internet est le but ultime de tout bidouilleur, car cela lui confère le moyen de lire, réacheminer, modifier ou effacer vos messages électroniques à votre insu. Certains bidouilleurs sont plus sélectifs et préfèrent les données des fournisseurs de services Internet ou les fichiers de sites Web comportant des numéros de cartes de crédit. D'autres s'intéressent aux secrets des entreprises ou aux renseignements personnels et tenteront de les obtenir pour les revendre ou les utiliser à mauvais escient.

Usenet

Un site Web peut aussi stocker, dans un dossier appelé « cookie », les renseignements relatifs à votre ordinateur, grâce auxquels il personnalisera votre accueil lors de votre prochaine visite à ce même site. Vous pouvez toutefois librement refuser le cookie.

Des municipalités et des organismes gouvernementaux s'intéressent de plus en plus à la communication au public de renseignements généraux par l'entremise du World Wide Web. L'intention est fort louable, mais le résultat ultime peut être désastreux. Par exemple, face à un tollé général, deux municipalités, pour ne nommer que celles-ci, ont dû revoir le contenu de leurs pages; il s'agit de Victoria (Colombie-Britannique) et d'Aylmer (Québec); cette dernière a dû retirer de ses pages sur les taxes foncières les montants dûs. Le registre des taxes foncières est un document public, mais il y a néanmoins tout un écart entre une consultation personnelle effectuée à l'hôtel de ville et la mise à la disposition de 50 millions d'internautes à travers le monde, contrairement installés chez eux, des coordonnées d'une personne, de la valeur de sa propriété, des taxes dues et (dans certaines administrations) de son affiliation religieuse. De même, la Société de téléphone du Manitoba a dû retirer de son site Web son système de facturation suite aux protestations de ses abonnés.

La participation à des groupes de discussions sur Usenet peut mener à une seconde forme d'abus de la vie privée, moins bien connue. Chaque message expédié à un groupe de discussion est archivé ou conservé en mémoire afin que d'autres personnes puissent le consulter. Votre opinion personnelle sur un sujet donné est conservée de façon permanente, et il est de plus possible d'interroger Usenet en vue de découvrir à quels groupes de discussions vous avez participé, pour établir votre profil d'intérêts (DejaNews, le logiciel d'archivage de messages, permet d'éliminer des messages sélectionnés.) Il y a pire, car on peut aussi découvrir à quel moment votre message est consulté par une adresse électronique donnée.

Notre rapport annuel 1995-1996 offrait certains trucs sur la façon de protéger notre vie privée sur les réseaux électroniques (*La vie privée dans le cyberspace : guide aux suiveurs*). Deux ans plus tard, l'Internet s'est commercialisé (au point que des gouvernements étudient les façons de taxer les achats qui s'y font), et la vie privée court encore plus de risques. On trouve actuellement quatre grands types d'invasion dans la vie privée sur l'Internet :

Sur le World Wide Web

L'invasion la plus considérable sur Internet est la collecte subreptice de vos renseignements personnels aux fins d'utilisation, de location ou de vente à des entreprises de marketing direct. Cela s'applique aux renseignements à votre sujet ainsi qu'aux renseignements sur vos activités sur le Web, par exemple :

- Votre adresse de courriel, quelquefois votre nom, l'adresse de votre protocole d'accès à Internet (grâce auquel un service de localisation de domaines peut vous situer géographiquement en gros), le genre de fureteur que vous privilégiez (et par là le système d'exploitation de votre ordinateur). Vous pouvez toutefois éviter de communiquer la plupart de ces renseignements en surtant d'abord des sites comme « Anonymizer » (www.anonymizer.com).

- On trouve, au nombre des renseignements concernant vos activités sur le Web, votre identité, la date de votre dernière visite au site, la dernière page que vous avez consultée (pour la fonction RETOUR de votre fureteur), les sections particulières du site que vous avez visité, combien de temps vous y avez passé, quels documents ou photos vous avez téléchargé, quels renseignements vous avez cherché avec des outils comme Alta Vista ou Yahoo. Vous pouvez toujours rendre anonymes les renseignements concernant votre « cliquage » en visitant d'abord certains sites.

En outre, le SCT semble considérer que le courrier électronique est nettement moins privé qu'une conversation téléphonique, puisque la politique envisage carrément sa surveillance sans le consentement de l'auteur ou du destinataire. Une surveillance similaire des conversations téléphoniques constituerait une infraction criminelle.

Les employés fédéraux ne sont pas tous parfaits; certains, comme leurs semblables du secteur privé, peuvent ne pas être productifs ou honnêtes dans leurs transactions. Toutefois, cela ne justifie pas qu'on fasse des employés fédéraux, dont la plupart agissent de façon responsable, la cible d'une surveillance sévère.

d'autres types de surveillance très envahissantes, comme de placer des caméras dans les toilettes, pourraient aussi être autorisés sur simple avis aux employés. Une telle interprétation (que nous supposons non intentionnelle de la part du SCT) pourrait éroder de façon grave et arbitraire le respect de la vie privée des employés du gouvernement. Nous n'affirmons pas que la surveillance des employés n'est jamais justifiée. Mais nous demeurerons très inquiets lorsque une politique confère à l'employeur un droit étendu à surveiller les activités électroniques des employés sans justification particulière.

Lors d'une rencontre avec le personnel du Conseil du Trésor pour discuter d'une ébauche préliminaire de la politique, nous avons soulevé plusieurs questions, dont les suivantes :

- Une politique gouvernementale qui autorise l'intrusion dans la vie privée sera certainement prise en exemple par le secteur privé pour justifier des politiques intrusives semblables. Elle ne devrait donc pas dépasser ce qui est absolument essentiel à l'atteinte des buts légitimes du gouvernement à titre d'employeur.
- Lorsqu'une intrusion est justifiée, il est préférable de recourir au départ à l'approche la moins intrusive. En d'autres termes, il vaut mieux commencer par éduquer en définissant clairement les utilisations acceptables des réseaux électroniques et celles qui ne le sont pas. Si cela ne permet pas de résoudre un problème, c'est seulement alors que l'on devrait recourir à des solutions de surveillance intrusives.

À partir de nos recommandations, le SCT a fait certains ajustements. Toutefois, la politique finale accorde toujours des pouvoirs excessifs sur le plan de l'intrusion. En particulier, le SCT semble avoir écarté notre suggestion proposant d'utiliser d'abord des mesures moins intrusives et d'adopter progressivement des mesures plus sévères seulement si les autres sont inefficaces. La politique envisage la surveillance du courrier électronique et des sites Internet visités, mais elle n'établit pas de limites suffisantes qui précisent à quel moment des mesures envahissantes peuvent être utilisées.

Politique du Conseil du Trésor sur l'utilisation des réseaux électroniques

Le gouvernement fédéral s'appuie de plus en plus sur les réseaux électroniques, tels Internet et le courrier électronique, pour la conduite de ses activités. Il a donc le souci de veiller à ce que les réseaux ne soient utilisés qu'à des fins gouvernementales et non à la poursuite d'activités illicites ou inacceptables.

En février 1998, le Secrétaire du Conseil du Trésor (SCT) a rendu publique sa nouvelle *Politique sur l'utilisation des réseaux électroniques*. Au nombre des obligations en découlant, le responsable d'un organisme est chargé d'élaborer un énoncé signalant aux employés qu'il est interdit de mener des activités illégales sur les réseaux du gouvernement et que certaines activités d'utilisation sont peut-être légales, mais qu'elles n'en demeurent pas moins inacceptables. Nous soustrivons à cette politique puisqu'un tel énoncé permettra de préciser les attentes de l'employeur et les droits des employés.

En vertu de la politique, un organisme est autorisé, à deux conditions, à signaler à un représentant officiel autorisé toutes les activités que l'on soupçonne être illégales : lorsqu'une plainte à cet égard est déposée, ou qu'une vérification de routine des réseaux électroniques (excluant la lecture du contenu des fichiers ou du courrier électronique) porte à croire qu'une personne utilise le réseau à des fins inacceptables. Une enquête peut donner lieu à une surveillance particulière ou à la lecture du contenu du courrier électronique et des fichiers.

La politique traite également des attentes de l'employé en matière de vie privée. On y note qu'en vertu de la *Charte des droits et libertés* un employé du gouvernement peut raisonnablement s'attendre à ce que sa vie privée soit respectée, même lorsqu'il utilise des ordinateurs gouvernementaux. Cependant, la politique laisse entendre que l'employeur peut diminuer chez l'employé cette attente raisonnable de respect de la vie privée en l'informant de ses activités de surveillance. On semble supposer que le droit de l'employé à une attente raisonnable de respect de sa vie privée doit être moindre si on lui signale que ses activités électroniques seront analysées. Si tel est le cas,

Vue la nécessité d'une politique et en raison du débat qui fait fureur, le gouvernement fédéral a publié un document de consultation à l'intention des Canadiens et a cherché à obtenir des commentaires dans trois domaines de politique : l'accès aux renseignements stockés, l'accès aux communications et les limites quant à l'exportation de produits de cryptographie faisant usage de clés de plus de 40 ou 56 octets.

Dans son mémoire, le Commissaire à la protection de la vie privée notait que l'interception élargie et les capacités de déchiffrement que voulaient les organismes responsables du maintien de l'ordre public ne constituaient peut-être pas la solution la plus appropriée aux problèmes de la criminalité et pourraient enfreindre la *Charte des droits et libertés*. De plus, ces organismes n'ont pas établi que les capacités d'interception et de déchiffrement recherchées mèneraient à une diminution des activités criminelles.

Le Commissaire recommandait aussi que :

- tous les Canadiens aient accès à la cryptographie;
- les Canadiens puissent choisir librement leur produit cryptographique s'ils souhaitent en utiliser;
- les Canadiens puissent décider librement comment traiter leurs clés cryptographiques;
- les clés cryptographiques et les informations chiffrées soient stockées de façon sécuritaire;
- toutes les activités de commerce électronique appuient la cryptographie.

Industrie Canada est en train d'étudier les réponses reçues sur le document de consultation.

mathématiques qui vont de 8 à plus de 2 000 octets de longueur (la plupart se situent entre 40 et 128 octets). Plus le nombre d'octets est élevé, plus la clé est sécuritaire parce qu'elle est plus longue à déchiffrer. Par exemple, la technologie actuelle permettrait de déchiffrer une clé de 56 octets en quatre heures mais quelques 10 billions d'années seraient nécessaires pour déchiffrer une clé de 112 octets!

D'un autre côté La cryptographie semble donc avoir résolu les problèmes électroniques de sécurité. Mais c'est là le hic, selon les

représentants officiels de l'ordre public; en effet, si la cryptographie permet de protéger vos communications en les chiffrant, les criminels y ont également accès. Les forces policières prétendent que, si elles ne peuvent pas accéder aux informations chiffrées et les déchiffrer, elles ne peuvent pas appliquer efficacement la loi. Les représentants de l'ordre public souhaitent donc que la cryptographie soit utilisée seulement s'ils ont accès aux clés de décodage des renseignements chiffrés. Cette suggestion n'est pas particulière au Canada, car plusieurs pays occidentaux industrialisés souhaitent l'application de semblables conditions et ont signé une entente (dite de Wassenaar) en vue entre autres de contrôler l'utilisation de la cryptographie.

Dans le cas présent, cependant, les intérêts des forces de l'ordre publique vont carrément à l'encontre des intérêts de la vie privée et des entreprises. Peu de gens souhaitent utiliser l'Internet pour acheminer des informations de nature délicate comme des renseignements médicaux, des numéros de cartes de crédit ou encore des secrets de marque déposés s'ils ne sont pas protégés. Cette suggestion revient un peu à demander à chacun de fournir à la police locale les clés de son domicile au cas où les policiers voudraient pénétrer sur les lieux.

L'étendue de l'accès proposé est sans comparaison et nous rapproche encore davantage d'un état policier. Cette proposition pourrait également s'avérer néfaste. En sachant que les communications électroniques ne sont pas protégées ou encore qu'elles sont sujettes à être interceptées par les forces de l'ordre publique, la confiance du public serait ébranlée et rendrait moins attrayants les projets comme le commerce électronique.

Peut-on garder un secret ?

À l'ère des ordinateurs, des appareils de communication personnels et des grands réseaux comme l'Internet, nous nous appuyons beaucoup sur une technologie non sécuritaire. À moins que nous ayons pris des mesures particulières, n'importe qui peut accéder à nos données et nos communications.

Heureusement, il existe aussi une technologie pour contrer l'interception non autorisée. Les données des communications vocales, du courrier électronique, des documents informatisés et des communications par télécopieur sont codées en cours de la transmission et de stockage par la technologie cryptographique. Même si elles accèdent au message, les tierces parties ne peuvent pas déchiffrer les informations sans le bon code. Le chiffrement permet aussi aux destinataires de confirmer l'identité de l'expéditeur et d'assurer que la communication n'a pas subi de modification au cours de la transmission.

Mécanisme cryptographique Il existe deux méthodes cryp-

tographiques, la cryptographie à clé secrète et celle à clé publique. La première utilise la même clé ou code pour chiffrer les données en une chaîne de caractères sans signification et pour les déchiffrer.

L'expéditeur et le destinataire doivent protéger leur clé.

La deuxième méthode, soit la cryptographie à clé publique, met à contribution une paire de clés différentes : une clé publique que l'expéditeur utilise pour transformer l'information avant de l'envoyer et une clé privée de décodage du message, connue seulement du destinataire. Seuls les renseignements transformés par la clé publique peuvent être déchiffrés par la clé privée correspondante. Cette méthode gagne en popularité en raison de sa facilité d'utilisation à grande échelle. La communication de la clé publique n'a lieu qu'une fois et équivaut à la publication d'un numéro de téléphone. La divulgation de notre clé secrète à tous ceux qui voudraient communiquer avec nous pourrait s'avérer fastidieuse et, une fois transmise, cette clé serait hors de notre contrôle.

L'efficacité d'un produit cryptographique repose sur la longueur des clés utilisées, comparabilisée en octets (un octet est une lettre ou un chiffre dans un mot). Les clés cryptographiques sont des formules

Le développement de nouveaux services (voir Internet – toujours pas de vie privée, à la page 71) pourrait très bien renforcer la vie privée des usagers. Toutefois, il est difficile d'en évaluer les avantages dans les communications électroniques puisqu'on en est encore aux premiers balbutiements. Il est sûr que les Canadiens devront s'informer davantage sur les technologies et les usages à mauvais escient auxquels leurs renseignements personnels peuvent être soumis. Lorsque nous comprendrons que les entreprises peuvent choisir d'utiliser la technologie de façon raisonnable ou irresponsable, nous serons alors en mesure de responsabiliser la gestion de ces entreprises plutôt que la technologie elle-même.

plus rigoureuse que les anciennes lignes directrices de l'OCDE, développées avant que le commerce électronique ne soit même envisagé. Un bon point de départ pourrait être la Directive de l'Union européenne sur la protection des renseignements personnels, qui entrera en vigueur en octobre 1998 et protégera la vie privée de plus de 350 millions de citoyens européens des secteurs public et privé. Le gouvernement fédéral veut être perçu comme un chef de file dans le domaine du commerce électronique mondial et est conscient que la confiance des Canadiens dans les réseaux est fondamentale à leur participation. Cependant, la mesure dans laquelle nous nous respectons les uns les autres est au coeur de l'interaction entre la technologie informatique et les renseignements personnels qu'elle traite. Nous savons que l'évolution de la technologie effrite le droit à la vie privée. Les mesures que le gouvernement fédéral a prises jusqu'à maintenant seront insuffisantes pour protéger la vie privée à cause des dangers inhérents au commerce électronique.

Examinons l'une des plus récentes méthodes de cueillette de renseignements personnels, soit la saisie de données expédiées par l'Internet. Chacun de nos mouvements et l'information que nous soumettons en ligne alimentent un prodigieux marché des renseignements personnels. Sans que nous le sachions et assurément sans notre consentement, un enregistrement est conservé de tous les écrans de chaque site Web visité. La collecte de ces données, communément appelées « flot de clics » (*clickstream*), permet de rassembler des renseignements sur tous les services et produits achetés en ligne. Mais ces bribes d'informations peuvent aussi être couplées avec vos habitudes de surfur du Web en vue d'établir un profil personnalisé de vos préférences et aversions — le rêve du marcatricien, ce spécialiste de la vente directe!

Il semble y avoir un consensus à l'effet que les personnes devraient être tenues de s'identifier lorsqu'elles veulent se procurer quelque chose par réseau. Toutefois, nombre de transactions que nous menons en personne demeurent anonymes, comme les achats au comptant. Le fait d'insister pour que nous révélions notre identité dans le commerce électronique mettrait fin à une longue tradition d'anonymat et mettrait en circulation des données nouvelles plus détaillées qui permettraient de suivre chacun de nos mouvements.

Le commerce électronique — Rêve de tout marcaticien... cauchemar pour la vie privée?

L'arrivée du commerce électronique a virtuellement transformé notre façon de magasiner et de faire des affaires. Règle générale, par commerce électronique, on entend des activités commerciales qui s'effectuent par des réseaux informatiques entre des personnes et des entreprises.

Il s'agit là d'un nouveau type de commerce qui offre des possibilités prodigieuses de rejoindre de nouveaux clients et de rendre les entreprises accessibles aux clients. Le gros du commerce électronique se concentre sur l'achat de services, tels les services bancaires en ligne, plutôt que sur des produits, mais les gouvernements et les entreprises à l'échelle mondiale s'activent sérieusement à élaborer un cadre pour l'achat électronique de biens.

Pour préparer le Canada au marché électronique, le gouvernement fédéral a publié récemment deux documents de travail. L'un a trait à la protection des renseignements personnels dans le secteur privé, et le second traite de la cryptographie aux fins du commerce électronique. Malgré ces initiatives, il reste beaucoup à faire pour protéger la vie privée des Canadiens. Pour plus d'informations, le lecteur est prié de passer aux pages 12 et 65 et à la réponse du Commissaire à ces initiatives.

Ces documents de travail et les initiatives proposées ont un échéancier serré. Ils sont partie intégrante de la préparation du gouvernement fédéral pour la conférence ministérielle que tiendra le gouvernement du Canada et l'OCDE en octobre 1998 à Ottawa. Heureusement, la protection de la vie privée est à l'ordre du jour. L'adaptation des lignes directrices de l'OCDE de 1980 sur la vie privée aux réseaux mondiaux actuels se poursuit également. L'OCDE compte présenter et faire adopter ces lignes directrices à la conférence d'octobre à Ottawa.

Les pays membres de l'OCDE qui tentent d'élaborer une protection efficace de la vie privée devraient étudier une initiative plus récente et

programmes sociaux, ce ministère détient la banque de données la plus considérable de tout le gouvernement fédéral. Il a également recours à beaucoup d'applications à la fine pointe de la technologie. L'examen de son rendement a exigé un effort de l'ensemble de tous les chefs de portefeuille, avec la contribution du personnel des politiques et de la recherche. Alors que la notion de portefeuille demeure valide, il n'en demeure pas moins qu'elle ne peut plus être la seule préconisée. Les chefs de portefeuille devront de plus en plus travailler à des questions cruciales, concernant un ministère ou encore l'ensemble du gouvernement.

En outre, le Commissariat a une poignée d'analystes en politiques et de chercheurs affectés à quatre autres activités principales, soit la surveillance des tendances et des développements au Canada et à l'étranger, la recherche de sujets d'intérêt précis ou urgents, le développement de positions et de politiques sur les nouvelles législations, les programmes et les questions centrales. De plus, la direction collabore de façon essentielle aux activités de communication que déploie le Commissaire lors de présentations et de discours aux organismes fédéraux et aux entreprises, en procédant à des entrevues avec les médias, en répondant aux demandes de renseignements, en surveillant les nouvelles lois et en préparant des soumissions aux comités parlementaires et aux organismes fédéraux et en participant à des projets conjoints impliquant le public et les agences du secteur privé. Ces activités pourraient très bien être celles qui ont eu le plus d'impact sur le public au cours des 16 ans d'existence du Commissariat.

Toutefois, à la vitesse où les changements sociaux et technologiques se produisent au Canada et à l'étranger, le Commissariat doit maintenant aller plus loin et faire converger ses travaux de recherche et de politique. La réponse privilégiée a été de jumeler le personnel des portefeuilles et celui affecté à la recherche et aux politiques afin qu'ils s'aident réciproquement. En gros, tout le contenu du présent rapport, à l'exception des plaintes particulières ou des questions juridiques, provient de cette section.

Fenêtre élargie sur les questions de vie privée

Le rôle principal du Commissaire à la protection de la vie privée est d'enquêter sur les plaintes concernant des présumées violations de la *Loi sur la protection des renseignements personnels*. Cependant, au mandat du Commissaire s'ajoutent deux autres composantes; il doit agir au nom du Parlement à titre de protecteur efficace de la vie privée et être pour le Parlement et les Canadiens une fenêtre ouverte sur les questions de vie privée.

Ces deux rôles exigent qu'il puisse évaluer professionnellement dans quelle mesure le gouvernement respecte les dispositions de la *Loi sur la protection des renseignements personnels* et que ses activités de recherche et de communication mettent à la disposition des décideurs et du public en général les faits permettant de rendre des jugements avisés dans le domaine de la vie privée. Ces deux responsabilités ont été regroupées en une seule direction, soit l'Analyse et gestion des enjeux et l'évaluation des pratiques équitables en matière d'information.

En 1994, à la suite d'une restructuration de toutes les institutions gouvernementales, l'ancienne Direction de la conformité a modifié sa façon de faire. Son faible effectif n'était plus en mesure de mener les vérifications passives courantes et d'effectuer le suivi. Une nouvelle direction a donc vu le jour pour se pencher sur les nouvelles lois et programmes et fournir des avis dynamiques et des conseils aux organismes fédéraux. Ceux-ci ont été regroupés en quatre secteurs d'activité principaux avec chacun un chef de portefeuille.

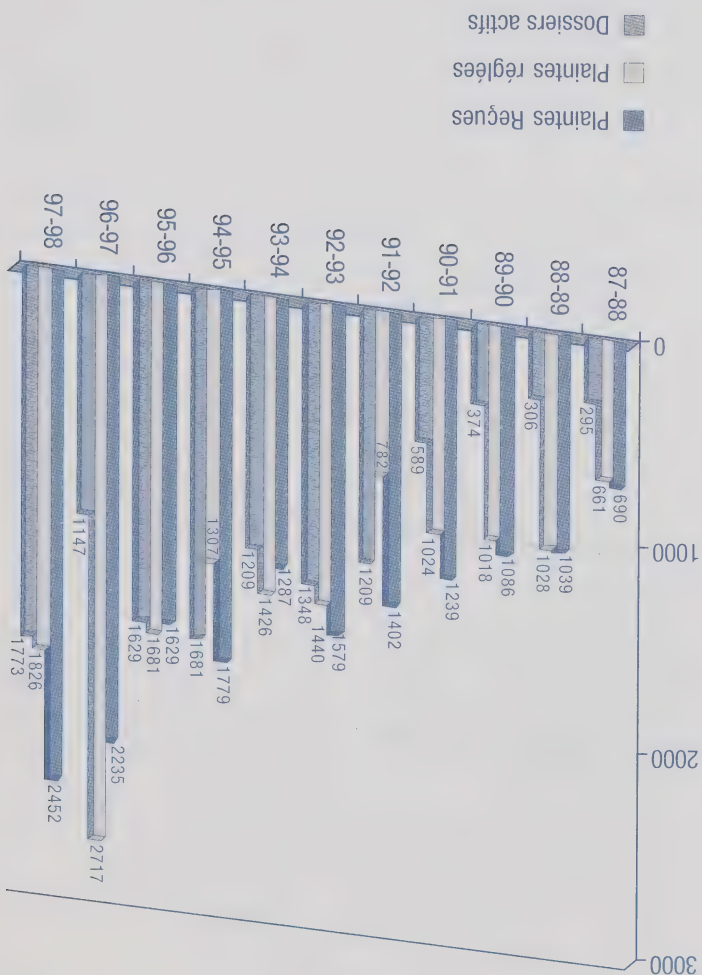
D'autres changements sont survenus au cours des quatre dernières années afin que le Commissariat puisse satisfaire à sa mission. L'expérience a démontré en effet aux chefs de portefeuille que tous les organismes regroupés dans leur portefeuille n'ont pas tous besoin de la même attention. De nouvelles questions d'importance exigeant la participation active des chefs de portefeuille oeuvrant en équipe avec un organisme ont récemment émergé au sein du gouvernement fédéral.

Un bon exemple en est la réorganisation toujours en cours de toutes les activités de Développement Ressources Humaines Canada (DRHC). En tant que gestionnaire et agent responsable de plusieurs

Origine des plaintes réglées

14	Terre-Neuve
2	Ile-du-Prince-Edouard
45	Nouvelle Ecosse
42	Nouveau-Brunswick
393	Québec
11	Région de la capitale nationale - Québec
276	Région de la capitale nationale - Ontario
504	Ontario
25	Manitoba
88	Saskatchewan
151	Alberta
253	Colombie-Britannique
2	Territoires du Nord-Ouest
20	Hors Canada
1826	TOTAL

Plaintes 1987-98

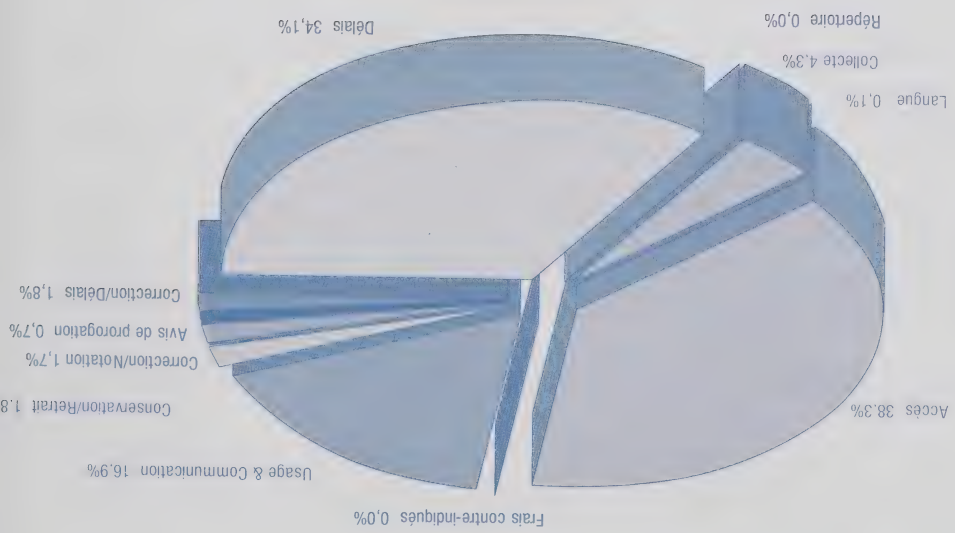


Le tableau reflète des variances minimales apportées aux statistiques pour les années 1993-94 à 1995-96

Plaintes réglées et motifs 1987-98



Plaintes réglées par motifs



Plaintes réglées par institutions et résultats

(suite)

Institution	Total	Fondée	Fondée: résolue	Non-fondée	Aban-donnée	Résolue	Réglée
Elections Canada	2	1	0	0	0	0	1
Environnement Canada	6	3	0	3	0	0	0
Gendarmerie royale du Canada	109	6	2	64	10	4	23
Industrie Canada	8	1	1	1	0	1	4
Justice Canada	40	12	6	8	4	2	8
L'Enquêteur correctionnel Canada	1	0	0	1	0	0	0
Patrimoine Canada	9	1	2	3	2	0	1
Pêches et Océans	2	0	0	1	0	0	1
Ponts Jacques-Cartier et Champlain Inc.	2	0	0	2	0	0	0
Ressources naturelles Canada	4	0	1	0	0	0	3
Revenu Canada - Impôt, douane et accises	293	156	1	65	28	15	28
Santé Canada	9	2	0	4	2	1	0
Service canadien du renseignement de sécurité	51	0	0	44	0	0	7
Service correctionnel Canada	373	124	24	109	33	25	58
Société canadienne d'hypothèques et de logement	2	0	1	1	0	0	0
Société canadienne des Ports	3	0	0	0	0	0	3
Société canadienne des Postes	53	0	4	23	4	9	13
Société d'assurance-dépôts du Canada	1	0	0	0	0	0	1
Société du crédit agricole Canada	2	0	1	0	0	0	1
Soliciteur général Canada	4	2	0	1	0	1	0
Statistique Canada	3	0	0	0	1	0	2
Surintendant des institutions financières Canada	2	0	0	2	0	0	0
Transports Canada	15	0	0	8	0	3	4
Travaux publics et Services gouvernementaux Canada	13	0	3	7	0	0	3
Vérificateur général du Canada	1	0	0	0	1	0	0
Voie maritime du Saint-Laurent, La	1	0	1	0	0	0	0
TOTAL	1826	638	126	547	128	76	311

Plaintes réglées par institutions et résultats

Institution	Total	Fondée	Fondée: résolue	Non-fondée	Aban-donnée	Résolue	Régée
Anciens combattants Canada	8	2	0	4	1	0	1
Affaires étrangères et Commerce int. Canada	16	4	0	5	4	1	2
Affaires indiennes et du Nord Canada	8	4	1	0	0	0	3
Agence canadienne de développement int.	6	1	1	3	0	0	1
Agence spatiale canadienne	1	0	0	1	0	0	0
Agriculture et Agro-alimentaire Canada	4	1	2	1	0	0	0
Archives Nationales du Canada	20	7	1	6	0	1	5
Banque du Canada	4	0	2	1	0	0	1
Banque fédérale de développement	2	0	2	0	0	0	0
Bibliothèque nationale du Canada	2	0	0	0	0	0	2
Bureau du Conseil Privé	7	2	0	2	0	0	3
Citoyenneté et Immigration Canada	95	28	41	9	5	0	12
Commissariat aux langues officielles	2	0	1	1	0	0	0
Commission canadienne des droits de la personne	3	0	0	2	0	0	1
Commission canadienne du blé	3	0	0	3	0	0	0
Commission d'appel de l'immigration	58	9	5	18	7	7	12
Commission de la fonction publique du Canada	10	6	0	2	1	1	0
Commission des plaintes du public contre la GRC	4	0	0	2	1	0	1
Commission des relations de travail dans la fonction publique	2	0	0	0	0	0	2
Commission nationale des libérations conditionnelles	30	2	6	11	5	2	4
Conseil de la radiodiffusion et des télécommunications canadiennes	4	0	0	4	0	0	0
Conseil du Trésor du Canada, Secrétariat	70	2	0	66	1	0	1
Conseil national de recherches Canada	1	0	0	0	0	1	0
Défense nationale	300	220	4	16	14	4	42
Développement des ressources humaines Canada	157	42	13	43	4	7	48

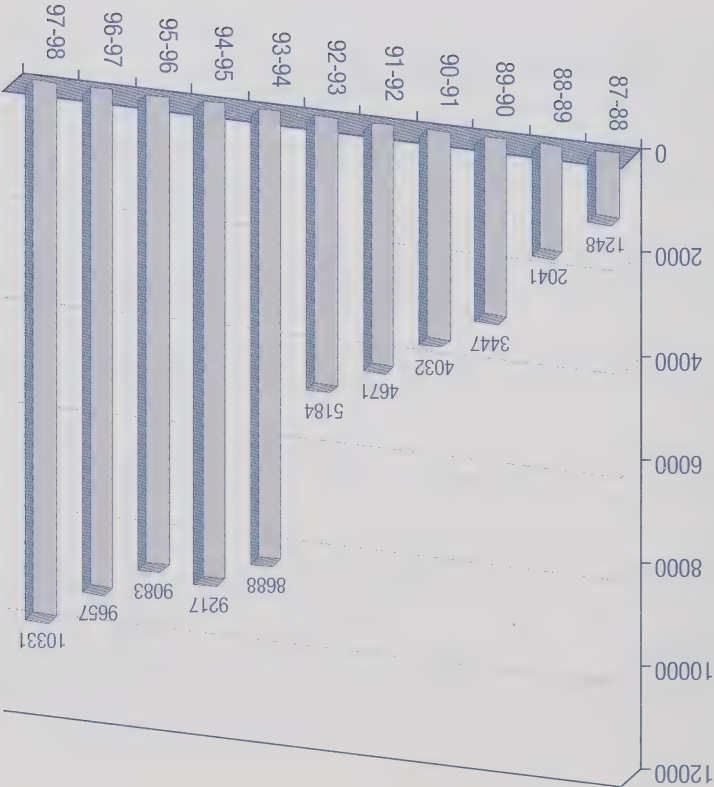
Plaintes réglées par motifs et résultats

Résultats							
Motifs	Fondée	Fondée; résolue	Non fondée	Aban- donnée	Résolue	Réglée	TOTAL
Accès	20	99	288	60	51	217	735
Accès	19	94	267	60	51	210	701
Correction/Annotation	1	4	20	0	0	6	31
Frais contre-indiqués	0	0	0	0	0	1	1
Répertoire	0	0	0	0	0	0	0
Langue	0	1	1	0	0	0	2
Atteinte à la vie privée	28	27	217	44	24	81	421
Collecte	2	8	35	4	10	20	79
Conservation/Retrait	6	0	12	7	0	8	33
Usage/Communication	20	19	170	33	14	53	309
Délais	590	0	42	24	1	13	670
Correction/Délais	31	0	1	1	1	0	34
Délais	559	0	29	22	0	13	623
Avis de prorogation	0	0	12	1	0	0	13
TOTAL	638	126	547	128	76	311	1826

Les dix ministères les plus visés selon les plaintes reçues

Motifs					
Ministère	TOTAL	Accès	Délais	Vie privée	
Développement ressources humaines Canada	781	69	41	671	
Revenu Canada	572	71	145	356	
Défense nationale	336	84	233	19	
Service correctionnel Canada	263	123	98	42	
Gendarmerie royale du Canada	95	65	10	20	
Citoyenneté et immigration Canada	69	30	28	11	
Justice, Ministère de la	59	34	22	3	
Service canadien du renseignement de sécurité	31	31	0	0	
Société canadienne des Postes	27	15	3	9	
Commission nationale des libérations	24	12	6	6	
AUTRE	195	95	50	50	
TOTAL	2452	629	636	1187	

Demandes de renseignements 1987-98



Loi - interprétation et application	4 812
Aucune compétence fédérale	358
Aucune compétence, secteur privé	401
Acheminées au commissaire provincial	810
Acheminées à un autre organisme fédéral	270
Acheminées ailleurs	74
Numéro d'assurance sociale	523
Institutions financières, assurance, crédit	327
Télécommunications	100
Marketing direct	42
Dossiers criminels, pardons, dérogations américaines	154
Médical	120
Adoption, généalogie, personnes portées disparues	97
Autres	726
Affaires publiques (médias, publications)	1517
TOTAL	10 331

Le tableau qui suit établit la ventilation des demandes de renseignements par catégories.

Demandes de renseignements par type

Dans son effort pour solutionner rapidement et de façon informelle les problèmes, les agents de requêtes ont été mis à contribution par le Commissariat. Ainsi, dans un cas précis, un député avait averti le Commissariat que les bureaux de Ressources Humaines de Terre-Neuve demandaient aux prestataires d'assurance-emploi venus réclamer leurs chèques au cours de la grève postale de signer un reçu sur lequel étaient inscrits les noms de tous les prestataires et les montants des chèques. Tous ceux qui venaient percevoir un chèque pouvaient voir quelles autres personnes étaient prestataires d'assurance-emploi et combien elles recevaient.

Les agents de requêtes ont confirmé la situation avec le personnel de DRHC et demandé qu'on intervienne rapidement. Il semble que cette pratique n'avait cours qu'à Terre-Neuve et dans la région de Windsor en Ontario. L'administration centrale de DRHC a averti les régions qui ont repris la pratique utilisée dans le reste du pays, soit d'émettre un reçu individuel. Le lendemain de l'appel, le problème était résolu.

Demandes de renseignements

Les demandes de renseignements consistent en appels et lettres qui n'entrent pas dans la définition de "plaintes" au Commissaire à la protection de la vie privée. Il peut s'agir de demandes pour obtenir des renseignements généraux et de publications sur la Loi, de plaintes impliquant des organismes auxquels la Loi ne s'applique pas, comme les sociétés de la Couronne, les gouvernements provinciaux et le secteur privé ainsi que des questions de vie privée qui dépassent la simple protection des renseignements personnels.

Au cours de l'année dernière, deux agents de requêtes ont traité 10 331 demandes allant de l'accès à des dossiers d'adoption aux divulgations de renseignements de crédit, en passant par la surveillance vidéo au coin des rues. Plusieurs appels concernaient le couplage des formulaires de déclaration des voyageurs de Douanes Canada aux données de l'Assurance-emploi, et quelques-unes demandaient conseil pour se présenter devant les juges et juges-arbitres. Le Commissariat ne peut fournir d'avis juridique aux personnes impliquées dans la démar-che mais le personnel a tout de même offert aux appelants une copie de la lettre précisant la position du Commissaire sur cette question.

L'expédition de la lettre de consentement pour les allocations de la C.-B. accompagnée d'un énoncé complet sur la cueillette (voir p. 90) nous a inondé d'appels, certains appelants demandant au Commissaire fédéral de passer outre au gouvernement provincial. Comme le Commissaire n'a pas compétence dans les affaires provinciales, les appels ont été réacheminés au commissaire provincial à la vie privée et à leur représentant parlementaire.

Plusieurs appels sont également parvenus à nos bureaux au sujet de la nouvelle brochure de la Banque Toronto Dominion. Des personnes protestaient contre le fait d'être contraintes de choisir de figurer ou non à ses projets de partage de leurs informations avec les autres filiales. Les clients avaient jusqu'en octobre 1998 pour faire part de leur préférence. S'ils ne se prononcent pas, la Banque conclura que les informations devraient être partagées. Alors que les défenseurs à la vie privée privilégient un consentement actif plutôt que passif, ce critère est conforme au critère de consentement du code de protection de la vie privée de l'Association des banquiers canadiens ainsi que celui de l'Association canadienne de normalisation sur lequel il a été modelé.

fondée par le Commissaire. Quoique satisfait des explications fournies par l'enquêteur, le plaignant est toujours frustré de voir que ni le CRTC ni le Conseil n'a encore effectué de suivi auprès de lui. Le CRTC juge que les questions de facturation concernent l'abonné et l'entreprise de câblodiffusion et a classé le dossier.

De nouveaux numéros personnels mettront fin à la divulgation du NAS aux syndicats

Une autre plainte ayant trait à l'omniprésence du NAS concernait sa divulgation au Syndicat des employés des postes par Postes Canada. La carte d'affiliation du membre au syndicat affichait le NAS et avait en plus été communiquée à une compagnie d'assurance.

L'enquêteur a rapidement établi que Postes Canada avait communiqué ces renseignements conformément aux termes de son entente collective avec le syndicat. Le NAS est utilisé par le régime de paie de Postes Canada et le syndicat maintient que celui-ci est nécessaire pour l'identification de ses membres dans le système informatique. En outre, les membres en bonne et due forme bénéficient d'une police d'assurance détenue par le syndicat et peuvent se prévaloir de couverture supplémentaire. Puisque l'administration de ce service est également reliée au régime de paie de Postes Canada, les membres du syndicat donnent nécessairement leur NAS à la compagnie d'assurance.

La Commission des relations de travail de la Fonction publique s'est prononcée à plusieurs reprises sur la question de la communication du NAS aux syndicats malgré les restrictions énoncées dans la *Loi sur la protection des renseignements personnels*. Néanmoins, le Commissaire s'inquiète toujours de la pratique et a encouragé le ministère de la Justice à faire appel d'un cas. Entre-temps, Postes Canada se convertit au numéro d'identification de DRHC en vue de remplacer le NAS. La conversion a été mise en veilleuse puisque Postes Canada se pré-paraît à affronter une grève. La divulgation prendra fin une fois la conversion faite.

La question de l'utilisation de ces numéros par les syndicats ou les compagnies d'assurance se situe hors du mandat du Commissariat.

À l'administration centrale de Citoyenneté et Immigration, on a mis en garde le consulat de Buffalo, ainsi que toutes les délégations à l'étranger, des risques de communications inappropriées de renseignements personnels encourus par l'utilisation des cartes postales. À la satisfaction du plaignant, le consulat a repris la pratique des lettres scellées. La plainte a été jugée résolue au cours de l'enquête.

Le CRTC réfile les plaintes de facturation du câble au Conseil de l'Industrie

Beaucoup de Canadiens ont l'impression que les plaintes portant sur le contenu d'émissions diffusées ou la facturation du câble relèvent du CRTC alors que ce n'est pas le cas. Cette situation a amené un Torontois à se plaindre de ce que le CRTC aurait communiqué de façon inappropriée au Conseil des normes du câble de la télévision, ainsi qu'à la compagnie de câble, sa plainte concernant une entreprise de câble locale.

Dans le cadre de sa réforme réglementaire de 1988, le CRTC avait encouragé les secteurs de radiodiffusion à régler eux-mêmes les questions ayant trait aux annonces subliminales et sexistes, à la violence, au contenu de la programmation pour enfants et aux loteries. Le secteur de la cablodiffusion devait également traiter de la facturation et des plaintes ayant trait au service.

On avait demandé aux secteurs de cablodiffusion de développer des normes et de soumettre celles-ci à l'approbation du CRTC. La conformité aux normes et la résolution des plaintes relevait des conseils propres à chaque domaine; ainsi la télévision par câble est sous la responsabilité du Conseil des normes de télévision par câble.

La plainte de l'individu au CRTC sur des irrégularités de facturation et l'impolitesse du personnel de la compagnie avait été acheminée au Conseil qui, à son tour, l'avait renvoyée à la compagnie de cablodiffusion. Celle-ci doit répondre par écrit au plaignant, qui peut porter le tout à l'attention du Conseil si les résultats obtenus ne le satisfont pas. En vertu du nouveau mécanisme, une telle divulgation permet à la compagnie de prendre connaissance de la situation, et au Conseil de voir à ce que les problèmes soient résolus. La plainte a été jugée non-

• autant que possible la surveillance vidéo clandestine ne devrait pas faire intrusion dans la vie privée d'autres personnes que la personne visée;

• la surveillance devrait se poursuivre seulement le temps nécessaire à la conduite de l'enquête;

• l'accès aux cassettes vidéos et à tout type d'information enregistrée doit être limité strictement à ceux qui ont un besoin légitime de l'information, et ces outils ne doivent pas être utilisés à titre de moyen pour, comme par exemple, surveiller en général le rendement d'un(e) employé(e);

• la personne sous surveillance vidéo clandestine doit être avertie après coup de la surveillance, y compris où et quand elle a eu lieu ainsi que ce qui a justifié la surveillance à moins de motifs valables de ne pas le faire.

Où l'utilisation de cartes postales peut susciter des divulgations concernant l'immigration

Devant les charges de travail et les délais, les fonctionnaires cherchent des façons plus rapides et efficaces de faire leur travail. Tout cela est bien sûr fort louable mais seulement en autant qu'on respecte les droits des individus. Ainsi, lorsque le consulat canadien à Buffalo, N.Y., a entrepris d'utiliser des cartes postales pour accélérer la réception de demandes d'immigration plutôt que par enveloppe scellée, un consultant de Toronto s'est plaint que l'utilisation de ces dernières identifiât la personne en tant que demandeur.

L'enquêteur a établi que le consulat avait été littéralement inondé avec quelque 5000 demandes soudaines d'immigration. Ce flot de demandes était attribuable au fait que des candidats tentaient de faire valider leurs demandes sous le régime des règlements antérieurs à ceux qui entraient en vigueur le 1^{er} mai 1997.

Pour accélérer la réception rapide des demandes, le consulat avait eu recours aux cartes postales sur lesquelles figuraient le nom du candidat, son numéro de dossier et une note à l'effet que "la demande de résidence permanente avait été reçue".

Selon le Commissaire, la Commission s'inquiétait à juste titre de fuites possibles et avait l'obligation de protéger les renseignements personnels, mais la méthode d'enquête utilisée était excessive en raison du manque de preuves. La plainte a été jugée fondée.

Recherche : politique gouvernementale sur la surveillance des employées

Le Commissaire a fait un pas de plus et écrit au Conseil du Trésor en insistant sur l'importance d'élaborer une politique gouvernementale élargie sur la surveillance clandestine des employés. Comme point de départ, il a communiqué les recommandations qu'il avait faites sur la question à la Commission de l'immigration et du statut de réfugié.

Ses recommandations étaient à la fois générales — concernant les enquêtes sur les employé(s) et d'ordre particulier. Toute politique sur la surveillance vidéo clandestine devrait satisfaire à *toutes* les exigences suivantes :

- des soupçons raisonnables doivent prévaloir avant d'opter pour une surveillance vidéo clandestine à titre de méthode d'enquête, dans le cas de sérieuses fautes de conduite graves, y compris des erreurs d'inconduite dans le domaine criminel;
- la surveillance vidéo devrait être utilisée strictement lorsque toutes les autres mesures raisonnables se sont révélées inefficaces ou jugées sans effet probable, y compris des méthodes de échange aux mesures d'enquêtes comme le counselling, les avis au lieu de travail, les programmes d'éducation;

- la surveillance vidéo devrait être utilisée lorsqu'on est en droit de s'attendre à un certain degré d'intimité, tel dans les salles d'habille-ment. Si la présomée conduite sur laquelle on enquête est, croit-on, de nature criminelle, on devrait demander aux forces policières d'enquêter. Ce faisant on s'assurera d'une révision judiciaire puisque les forces policières doivent d'abord obtenir un mandat les autorisant à effectuer une surveillance vidéo clandestine là où un individu est en droit de s'attendre à un peu d'intimité.

- là où les personnes ne sont pas en droit de s'attendre à un certain degré de respect de leur vie privée, seul le responsable de l'institution gouvernementale devrait avoir l'autorité d'ordonner la tenue d'une surveillance vidéo clandestine, et ne devrait pas déléguer celle-ci;

Inquiets de la fuite de renseignements et de l'existence possible d'une source à l'intérieur, le personnel de la Commission responsable de la sécurité a entrepris une enquête interne. Se fiant à la description fournie par la réfugiée, il a procédé à l'identification d'une employée correspondant à la description obtenue; il s'agissait en l'occurrence d'une commis d'un bureau régional. Les cadres supérieurs de la Commission ont approuvé l'utilisation d'une caméra, qui est demeurée en place jusqu'à ce qu'un technicien des Travaux publics la déloge devant l'employée en déplaçant quelques tuiles du plafond lors d'un entretien régulier. La Commission l'avait alors enlevée.

Le Commissaire a conclu que les éléments de preuve étaient insuffisants pour justifier une surveillance aussi intrusive car ils consistaient, en fait, en un oui-dire et le fait que l'employée et la tierce personne se connaissaient. L'enquêteur a déterminé que le personnel affecté à la sécurité n'avait jamais envisagé de confronter ou de consulter l'employée en question. Par ailleurs, on peut s'interroger sur le genre de renseignements pertinents qui auraient pu être recueillis en braquant une caméra vidéo (sans son) sur le bureau de la commis. On peut supposer qu'un employé souhaitant communiquer l'information subrepticement ne le ferait pas sur les lieux de son travail et à la vue de tout le monde. En outre, la caméra n'aurait pas permis d'écouter les appels téléphoniques compromettants.

Le Commissaire s'est interrogé sur le fait que la Commission ait recouru à la surveillance clandestine sur un simple soupçon. Selon lui, on ne devrait recourir à la surveillance que lorsqu'une enquête préliminaire a permis d'établir qu'un employeur est en droit de soupçonner un employé d'inconduite, et encore on ne devrait considérer cette possibilité que lorsque toutes les autres techniques d'enquête auraient été épuisées ou jugées inefficaces. Le Commissaire a demandé à la Commission de lui communiquer ses observations. La Commission a admis qu'en rétrospective, une enquête par un organisme responsable de l'application de la loi aurait été préférable. Elle a offert ses excuses à l'employée et a entrepris l'ébauche d'une politique pour guider les employés dans ce genre de situations à l'avenir. Le Commissaire estime l'intention louable, mais il a tenu à faire plusieurs recommandations sur des points bien précis. (Voir ci-dessous.)

Il n'y a pas de raison valable pour qu'un employeur s'inquiète de la routine quotidienne d'un employé en congé sans solde puisqu'il ne peut pas abuser du système. Même la surveillance d'employés actuels avec solde serait difficilement justifiable puisque les employeurs n'ont pas le droit de dicter à leurs employés comment vivre leur vie privée. Le Commissaire a décrit les entrées du journal comme une forme de surveillance menée sans justification par le ministère. La plainte a été déclarée fondée.

Dans le cadre du processus de résolution du grief de la dame, le ministère a accepté d'enlever et de détruire les renseignements de ses dossiers administratifs. Cependant, les représentants du ministère ne voulaient pas enlever la documentation de leurs dossiers sur la vie privée, prétextant que ceux-ci devraient être conservés au moins deux ans après le dernier geste administratif, soit la résolution de sa plainte.

Ce délai de deux ans est le minimum prévu afin de permettre aux personnes d'avoir raisonnablement le temps d'accéder aux renseignements personnels que détient le gouvernement à leur sujet. Puisque dans un premier temps, les renseignements n'auraient pas dû être recueillis et que la plaignante en avait pris connaissance et souhaitait qu'ils soient éliminés, le Commissaire a insisté pour que le ministère accepte la demande de la plaignante. Éventuellement le ministère y a consenti et le Commissaire considère la question réglée.

Surveillance vidéo particulièrement intrusive et injustifiée

Au nombre des mesures dont disposent les employeurs, la surveillance clandestine est probablement l'outil le plus intrusif et celui qui doit être le plus étroitement contrôlé. Une plainte déposée contre la

Commission de l'immigration et du statut de réfugié illustre bien.

L'avocat d'une candidate au statut de réfugié a déclaré que quelques heures après la comparution à huit clos de sa cliente, une tierce personne avait déclaré à la réfugiée que sa demande avait été approuvée. La dame a fourni une description d'un employé de la Commission qu'elle avait aperçu en compagnie de la tierce personne. L'avocat a déposé une plainte auprès de la Commission.

modèle pour ses dispositions de contrat. En bout de compte, le contrat entériné à l'automne 1997 assujettissait la compagnie d'assurance au code de protection de la vie privée de l'Association canadienne de normalisation. Selon le contrat, les individus peuvent accéder à leurs dossiers et restreindre la communication de renseignements personnels à leur employeur (sauf lorsqu'il y a recours judiciaire, fraude ou vérification).

Parcs Canada joue à la bonne d'enfants

Une Albertaine s'est plainte au Commissaire à l'effet que Parcs Canada (partie de Patrimoine canadien) avait avait demandé à son surveillant de surveiller ses allées et venues alors qu'elle était en congé sans solde pour s'occuper de son enfant.

Des mentions de ses déplacements, y compris ses visites à un voisin du surveillant, à un musée et à un poste d'essence local, ainsi que la présence ou non de son enfant à ses côtés figuraient dans le cahier de travail du surveillant de la plaignante. Il semble que le gestionnaire des ressources humaines avait ordonné au surveillant d'enregistrer ces détails parce que la dame était considérée comme une employée causant des problèmes.

On a pris connaissance de cela lorsque la dame a fait une demande d'accès formelle à ses renseignements personnels après qu'un enquêteur à la vie privée le lui eût suggéré. Plusieurs demandes informelles précédentes de consultation de son dossier n'avaient pas eu les résultats anticipés quant aux documents qu'elle croyait devaient y figurer.

Le fait que le comportement de la dame ait été documenté demeure un mystère. En effet, un congé sans solde est accordé en vertu de la convention collective de la fonction publique et ne peut pas être refusé. Les emplois des personnes ne sont pas conservés pendant ce genre de congé (mais on leur accorde priorité pour les emplois disponibles s'ils choisissent de réintégrer le travail). Selon Parcs Canada, parce que l'employée s'était vue accorder un congé parental, le ministère avait la responsabilité de s'assurer qu'elle s'occupait effectivement de son enfant, et expliqua ainsi son incursion plutôt inusitée dans la vie privée de l'employée.

nouveau régime à la Mutuelle du Canada, compagnie d'assurance sur la vie. En vue de rationaliser les coûts, le Conseil avait préconisé l'utilisation de la pharmacie postale pour économiser sur les frais d'ordonnance et les prix des médicaments. Les soumissionnaires retenus sont Meditrust et la Pharmacie Marcel Dubuc.

Afin de publiciser ce nouveau service, le Conseil a demandé aux pharmacies conçues de fournir des documents d'information et des enveloppes vierges à la Mutuelle du Canada et aux syndicats de la fonction publique. Les syndicats ont alors expédié la documentation à leurs membres, et la compagnie Mutuelle du Canada en a fait de même avec les participants au Régime qui avaient déjà soumis une réclamation médicale depuis la prise en charge du programme par la compagnie.

Le Commissaire est parvenu à la conclusion qu'il n'y avait pas eu de divulgation inappropriée de renseignements puisqu'on n'avait pas communiqué les noms et adresses des employés aux pharmacies. Il s'est cependant inquiété du fait que l'ancien régime de soins de la santé ne contenait aucun article relatif à la protection de la vie privée. Comme le Conseil du Trésor était en train de réviser le contrat, il en a profité pour demander qu'on y incorpore des mesures adéquates sur le contrôle gouvernemental et l'accès des individus aux données médicales.

Au cours des mois où l'enquêteur a négocié avec le Conseil du Trésor, le Conseil national mixte a réévalué son appui au programme de pharmacie postale. En mars 1997, il a informé ses membres qu'en raison du faible nombre d'adhérents au programme, les économies anticipées n'avaient pu se concrétiser. N'ayant pas prévu une utilisation aussi peu enthousiaste des pharmacies postales, le Conseil a mis fin à l'initiative. Le manque de conviction du personnel du Conseil du Trésor quant à l'utilité de dispositions relatives à la vie privée est responsable de la lenteur dans les progrès. En outre, le nouveau gérant du régime de soins de la santé, la compagnie d'assurance Sun Life du Canada, n'avait pas pris en considération les coûts de mise en oeuvre des dispositions.

Le personnel du Commissariat, à qui on avait demandé de revoir les dispositions proposées au cours de l'été suivant, a suggéré que Sun Life, qui adhère aux lignes directrices de l'Association canadienne pour la vie et l'assurance-santé en matière de vie privée, s'y réfère à titre de

familial, sont admissibles à ces allocations et il expédie mensuellement les chèques. Enfin, Revenu Canada transmet les noms et adresses des prestataires au gouvernement de la C.-B. lequel envoie à son tour, afin de gagner une certaine image à l'échelle provinciale, des avis aux familles qui sont admissibles.

Le partage limité de renseignements a eu lieu en vertu d'une entente provisoire alors qu'on ébauchait un protocole d'entente permanent. La *Loi sur l'impôt* autorise Revenu Canada à communiquer aux provinces des renseignements sur les contribuables pour l'administration d'une loi d'une province pour laquelle il recueille de l'impôt, ainsi qu'aux représentants officiels des provinces autorisées à recevoir les paiements. La *Loi sur la protection des renseignements personnels* permet précisément ce type de partage en vertu d'une entente ou d'un arrangement entre le gouvernement du Canada et le gouvernement de la province (alinéa 8(2) f). Par ailleurs, il autorise les communications permises dans toutes les autres lois du Parlement.

Le Commissaire a conclu que ce partage de renseignements était permis et que la plainte n'était pas fondée.

Noms et adresses non divulgués à des pharmacies postales

Vers la fin de 1995, de nombreux fonctionnaires ont reçu dans leur courrier des lettres personnalisées annonçant les services d'une pharmacie postale. Les lettres de Meditrust ou (au Québec) de la Pharmacie Marcel Dubuc se situaient dans le cadre d'une entente survenue avec le Régime de soins de santé de la fonction publique fédérale et offrait aux participants au régime l'option de se procurer par la poste leurs médicaments prescrits.

Au cours des semaines subséquentes, 65 employés ont porté plainte auprès du Commissaire à l'effet qu'on avait communiqué leurs nom, adresse et statut d'employé aux entreprises, et leurs soupçons portaient sur leurs employeurs.

L'enquête a établi qu'en août 1991, le Conseil national mixte (gestion et syndicats) avait suggéré des changements au régime de santé des employés en vue de le rendre auto-suffisant. Le Conseil du Trésor (l'employeur des fonctionnaires) avait alors accordé le contrat pour le

vie privée (ou à toute autre loi), l'enquêteur a demandé une démonstration du système de facturation électronique à une pharmacie de son quartier.

Le pharmacien inscrit tous ses clients dans son système informatique. Lorsqu'un aîné fait remplir une prescription, le pharmacien procède à son identification, inscrit la somme de 6,10 \$ ainsi que le prix du médicament, et transmet tous ces renseignements à la banque de données du Programme de médicaments gratuits de l'Ontario. Là, on confirme le montant que le client doit payer : le plein montant de la prescription, le montant de 6,10 \$ si la limite de 100 \$ a été atteinte, ou 2,00 \$ si l'aîné est subventionné. Le pharmacien peut certes déduire le revenu global de l'aîné en fonction du montant que ce dernier doit assumer, mais il n'a pas accès aux détails de son revenu.

Revenu Canada partage certains renseignements avec la C.-B. pour les allocations familiales

Les renseignements financiers, surtout ceux ayant trait à l'impôt sur le revenu, sont de nature très délicate. Des plaintes sont déposées dès qu'on soupçonne Revenu Canada de partager des renseignements fiscaux, même si c'est avec un gouvernement provincial. Une divulgation de Revenu Canada a amené un député à porter plainte pour lui-même et pour un de ses électeurs. Revenu Canada aurait communiqué des renseignements fiscaux à la Colombie-Britannique afin d'établir qui était admissible aux allocations familiales de la province. Le régime, qui est lié au revenu, vise à aider les familles à faible revenu qui ont des enfants à charge. On avertit les résidents de la C.-B. qu'ils n'ont pas à demander l'allocation puisqu'elle leur parvient automatiquement d'après le revenu familial inscrit sur la déclaration d'impôt annuelle.

En vertu d'ententes entre toutes les provinces (à l'exception du Québec) et le ministère des Finances, Revenu Canada assume la gestion de l'impôt sur le revenu. Il administre aussi entièrement le régime d'allocations familiales de la C.-B.; il identifie grâce à une formule pré-déterminée les familles qui, en vertu de leur revenu

En janvier 1996, le ministère des Finances de l'Ontario a demandé à DRHC si l'entente de 1976 incluait le partage de l'information pour le nouveau régime de médicaments basé sur le revenu. DRHC a répondu que les renseignements pourraient être utilisés aux fins stipulées dans l'entente originale. Le ministère de la Santé de l'Ontario a donc conclu que le but était identique, et a utilisé la bande informative de l'assurance-maladie de l'Ontario pour le programme de médicaments de l'Ontario. En août 1996, DRHC a déterminé que la nouvelle utilisation qui en était faite n'était pas conforme à l'entente de partage en vigueur.

Plusieurs rencontres ont eu lieu pour en venir à une nouvelle entente. Puis le processus a été mis en veilleuse en attendant que les parties en cause s'entendent précisément sur les renseignements qui sont nécessaires à la province pour l'administration du nouveau programme. Si DRHC n'avait pas systématiquement transmis de renseignements sur les paiements de la sécurité de la vieillesse et sur le supplément du revenu garanti, il est certain qu'une nouvelle entente aurait du survenir avant le lancement d'un programme relié au revenu. Sans ces informations, l'Assurance-maladie de l'Ontario n'aurait pas été en mesure d'établir précisément qui satisfaisait aux exigences en matière de revenus.

Il est également évident que DRHC a systématiquement divulgué des informations inutiles sur les prestations, et que les personnes n'ont pas été averties.

Dans le cadre de la résolution des plaintes, DRHC a non seulement cessé le transfert de renseignements au ministère de la Santé, mais a aussi abrogé l'entente de partage de 1976 autorisant le ministère des Finances de l'Ontario à divulguer des renseignements au ministère de la Santé, et a modifié son formulaire de sécurité de la vieillesse et du supplément de revenu garanti, de même que sa documentation à l'intention des requérants, pour y expliquer le partage des renseignements avec la province.

Les plaignants s'inquiétaient surtout du fait que les pharmaciens devaient connaître leur revenu afin de les facturer correctement. Quoique les pharmacies ne soient pas assujetties à la loi fédérale sur la

à 24 175 \$ doivent déboursier des frais d'administration de 2 \$ par ordonnance. Quant aux personnes ayant des revenus plus élevés, elles doivent déboursier annuellement un montant initial de 100 \$, ainsi que 6,11 \$ par ordonnance subséquente.

C'est lorsque les personnes âgées réclament le supplément de revenu garanti ou encore l'allocation au conjoint que DRHC obtient les renseignements en question. Parce que ces prestations ont trait au revenu, le formulaire demande le revenu de la personne âgée et précise que Revenu Canada vérifiera l'information en vertu d'une entente de partage de l'information. Le couplage n'est pas décrit dans Info Source comme le stipule la politique sur le couplage de données ou encore les déliants d'information du programme. Info Source décrit le couplage avec les provinces comme un usage compatible.

En vertu d'une entente de partage des données remontant à 1975, DRHC communiquait mensuellement au ministère des Finances de l'Ontario les listes informatiques provinciales du Supplément du revenu garanti. Cette entente était autorisée en vertu de la *Loi sur la prestation de la sécurité de la vieillesse* pour administrer les programmes sociaux, d'aide au revenu et d'assurance-santé. Cependant, l'entente indiquait que les renseignements ne devaient être utilisés que pour le supplément annuel de revenu garanti. L'année suivante, l'entente a été modifiée afin de permettre au ministère du Revenu de l'Ontario de communiquer des renseignements au ministère provincial de la Santé pour l'émission aux aînés de cartes d'assurance médicale donnant accès gratuitement aux médicaments.

À des fins pratiques, DRHC a entrepris de communiquer des copies informatiques distinctes au ministère des Finances de l'Ontario pour le supplément annuel de revenu garanti ainsi qu'au ministère de la Santé pour l'assurance-santé de l'Ontario. Puisque la carte de médicaments était à la disposition de toutes les personnes âgées, la liste pour l'assurance-santé comprenait tous les prestataires de la sécurité de la vieillesse et non pas seulement ceux à faibles revenus et incluait en outre la date de naissance, le sexe, la langue, le nas, la date de décès et les montants de la sécurité de la vieillesse ainsi que tous les autres suppléments reçus pour l'année en cours. Aucune autre information n'était offerte.

L'enquêteur a pu établir que, malgré les soupçons, Revenu Canada n'avait pas communiqué au ministère albertain des renseignements concernant certains requérants qui n'avaient pas rempli de déclaration de revenus mais qui en avaient reçu tel un montant minimal d'intérêt pour un compte d'épargne.

L'enquête a amené l'organisme à purger ses dossiers de 1993 et 1994 des renseignements fiscaux qu'ils contenaient, et à geler, puis à détruire en décembre 1997 des données de 1995. Revenu Canada ne communiquait plus que le strict minimum de renseignements et procédait aux vérifications de routine des dossiers des personnes pour s'assurer qu'elles sont consentantes.

Le Commissaire a jugé que les plaintes contre Revenu Canada étaient fondées. Cependant, en éliminant les données, en amendant son entente, en limitant le nombre de divulgations à venir et en vérifiant périodiquement les formulaires de consentement, le ministère a agi efficacement pour éviter que ceci se reproduise. Le Commissaire a cependant rejeté la plainte à l'effet que le formulaire de l'organisme ne constituait pas un consentement valide en vertu de la Loi sur la protection des renseignements personnels.

Programme de médicaments gratuits de l'Ontario

Suite au lancement du programme qui finance le coût des médicaments pour personnes âgées à faibles revenus, le Commissaire a été saisi de 25 plaintes de divulgation de renseignements personnels par le gouvernement fédéral au gouvernement de l'Ontario et, par l'entremise du système informatique, aux pharmaciens qui répondaient aux ordonnances des personnes âgées. Certains plaignants nommaient Revenu Canada alors que d'autres identifiaient DRHC. L'enquêteur a déterminé rapidement que Revenu Canada avait été approché par le gouvernement de l'Ontario, mais avait refusé de communiquer les données fiscales des personnes à moins que celles-ci n'y consentent. L'attention s'est alors portée vers DRHC.

C'est en juillet 1996 que les informations sur l'état des revenus sont devenus essentielles, soit lors de l'entrée en vigueur du nouveau régime. Actuellement, les personnes âgées ciblées disposant d'un revenu inférieur à 16 018 \$, et les époux ayant des revenus inférieurs

signer une disposition autorisant Revenu Canada à effectuer la divulgation. Le ministre albertain a conservé les formulaires et, à compter de novembre 1994, a soumis une demande en vrac à Revenu Canada utilisant les numéros d'assurance sociale des aînés concernés.

Malheureusement l'organisme n'a pas vérifié si tous les consentements avaient été obtenus et a tout simplement soumis la liste entière des demandeurs à Revenu Canada. Au nombre des 60 000 demandes vérifiées, sur un total de 194 000, 4 000 ne comportaient pas de consentement — 12 refusaient carrément d'y souscrire — dont plusieurs ont porté plainte auprès du Commissaire à la vie privée de l'Alberta, Bob Clarke. En raison des répercussions pour un si grand nombre de personnes âgées, les plaintes ont été regroupées en une seule plainte globale, parrainée par l'*Alberta Council on Aging* et portée à l'attention des deux commissaires, provincial et fédéral.

Les deux commissaires ont suivi la piste et se sont rencontrés à mi-chemin. M. Clarke s'est penché sur la collecte des formulaires de l'organisme et la demande à Revenu Canada. À notre bureau, nous avons enquêté afin de déterminer si effectivement Revenu Canada avait divulgué des renseignements fiscaux sans consentement préalable, si l'on en avait divulgué plus que nécessaire et si le formulaire d'autorisation de communication de Revenu Canada à l'organisme satisfaisait aux exigences de la *Loi sur la protection des renseignements personnels*.

L'enquêteur fédéral a établi que la première condition de l'entente fédérale-provinciale n'avait pas été respectée; l'organisme n'avait pas obtenu d'autorisation en bonne et due forme avant l'acheminement des renseignements à Revenu Canada. Revenu Canada pour sa part avait présumé que toutes les personnes dont les noms figuraient sur la liste étaient consentantes et avait donc répondu à toutes avec un imprimé normalisé de 75 rubriques. Il est évident que Revenu Canada a divulgué de façon irrégulière des renseignements en présumant que l'organisme avait respecté son engagement.

Il est cependant évident que Revenu Canada a communiqué beaucoup plus de renseignements que nécessaire pour obtenir confirmation du revenu du requérant, soit 75 lignes de données plutôt que 12. Les 75 lignes comprenaient la ventilation détaillée des sources de revenu et les exemptions (y compris : les pensions, dons et frais médicaux).

a manqué de transparence à l'égard des répondants en ne leur communiquant pas les motifs de la collecte des renseignements et comment ceux-ci seraient utilisés. La plainte a dont été jugée fondée.

Divuligation de renseignements fiscaux : pas sans le consentement du contribuable

Suite à l'inauguration de nouveaux régimes de prestations aux aînés de l'Alberta et de l'Ontario, de nombreuses plaintes ont été déposées à l'effet que le gouvernement fédéral divulguait aux organismes provinciaux gérant ces régimes des renseignements fiscaux sur les personnes concernées. Comme le revenu des demandeurs détermine les prestations des deux régimes, les agences provinciales désiraient que la source la plus fiable, en l'occurrence les dossiers d'impôt, confirme ces revenus.

Revenu Canada entérine des ententes avec les organismes gouvernementaux provinciaux pour la divulgation de certains renseignements fiscaux précis, mais seulement avec le consentement des contribuables. Au nombre des questions que les plaintes ont soulevées, nous retrouvons :

- Avait-on obtenu le consentement des contribuables?
- Revenu Canada était-il à la source des renseignements communiqués?
- Les divulgations de renseignements personnels avaient-elles été limitées au strict minimum requis pour l'atteinte des objectifs des programmes?

Le programme de prestation aux aînés de l'Alberta

Ce programme accorde certaines prestations aux personnes âgées dont le revenu est inférieur à la norme fixée par le *Alberta Ministry of Community Development*, qui gère le programme.

Dans le cadre d'un protocole d'entente survenu en octobre 1994, Revenu Canada et le ministère albertain ont convenu du transfert électronique de quantités importantes de renseignements sur les contribuables en autant que les personnes affectées fournissent une autorisation écrite en bonne et due forme. Les demandeurs devaient

Les répondants peuvent se consoler en sachant que les intervieweurs subissent une vérification approfondie de la fiabilité (y compris des antécédents criminels) et sont assujettis aux mêmes obligations que tous les employés de Statistique Canada. Ils portent une carte d'identification qu'on peut vérifier en composant le numéro qui paraît sur la carte.

L'identité des personnes n'est pas inscrite dans le fichier de données et les informations sont codées avant d'être transmises à Ottawa. À ce stade, les questionnaires sont expédiés aux archives du ministère après que le personnel en ait détaché la partie concernant les renseignements sur le ménage. Le seul lien entre le document sur papier et les données est un numéro d'identification sur le questionnaire qui pourrait permettre de remonter aux réponses sur support papier. Cependant, Statistique Canada n'a pas d'intérêt à identifier les répondants, sauf à des fins de vérification des données.

L'objectif visé, soit l'augmentation de la participation, a été atteint (augmentation de 12 pour cent) en déclarant le sondage obligatoire, mais a terni un tant soit peu la fiabilité des statistiques recueillies puisque certains répondants insatisfaits ont fait preuve de moins de candeur (ou ont été moins en profondeur). Statistique Canada a décidé de revenir à la participation volontaire au prochain sondage et à compter en augmentant à 27 000 l'échantillonnage des foyers participants.

Malheureusement, la brochure promotionnelle du nouveau sondage sur les dépenses des ménages fait preuve de moins de transparence quant aux avenues juridiques qui s'offrent aux répondants choisis. La lettre d'avis précise aux répondants que l'intervieweur leur rendra visite et demande leur collaboration pour remplir le questionnaire mais n'explique pas que la participation est volontaire. Le dépliant accompagnant la lettre précise que la participation est volontaire et souligne qu'il est important que tous les foyers sélectionnés participent. Elle ajoute que l'intervieweur se rendra aux domiciles des personnes et qu'ils rempliront ensemble le questionnaire. On n'y mentionne aucune autre option.

Le Commissaire a conclu que quoique Statistique Canada ait indéniablement le droit de mener ce sondage sur les dépenses familiales, il

poche et les brochures. Dans la catégorie des revenus, on demande la valeur des cadeaux reçus de personnes non apparentées.

On peut se demander combien de Canadiens se rappellent réellement en détail ces dépenses un an plus tard, mais l'énoncé de la *Loi sur la statistique* confère à Statistique Canada le pouvoir d'exiger des réponses. L'enquêteur a dû rapidement décevoir les plaignants qui croyaient que le Commissaire pouvait les soustraire à cet exercice. Cependant, il y a eu des aspects du processus qui nécessitaient des éclaircissements, surtout en ce qui a trait à la transparence.

Tout d'abord, il y avait la conduite du sondage sous forme d'entrevues. Cela exigeait des répondants qu'ils confient des détails personnels à un parfait étranger plutôt que de simplement compléter un formulaire à leur gré. Il est évident que Statistique Canada préfère les entrevues personnelles afin de clarifier les questions, d'obtenir des réponses et de s'assurer que le questionnaire est rempli. Le ministère se préoccupe aussi de la qualité des données. Cependant, en répondant simplement au questionnaire, le répondant satisfait à ses obligations légales et Statistique Canada pourvoit à ses besoins. Les personnes qui se sentent en mesure d'y répondre elles-mêmes devraient dès le départ se voir offrir l'option de pouvoir le faire.

Un second sujet de préoccupation était l'exigence apparente que l'entrevue ait lieu au domicile du répondant. Des lettres avisant les forces policières locales, les politiciens et les gérants de propriétés résidentielles du sondage à venir (au cas où il y aurait des appels) signalaient clairement que les intervieweurs comptaient visiter les répondants à domicile. Cependant, la lettre d'avis au répondant était moins précise et leur signalait qu'un intervieweur se présenterait en vue de les aider pour cette étude importante.

Devoir répondre à des questions aussi détaillées chez soi peut sembler très envahissant. Selon Statistique Canada, les intervieweurs auraient été disposés à rencontrer les répondants ailleurs, mais comme la plupart des gens auraient eu besoin de consulter leurs dossiers pour compléter le questionnaire, la préférence allait nettement en faveur de l'entrevue à la maison. Malgré tout, les répondants ne sont clairement pas forcés d'accepter.

ou louché, à la composition des ménages ou à d'autres aspects choisis de ceux-ci. Les entreprises sont alors en mesure de cibler des groupes particuliers.

À moins que le ministre n'en décide autrement, chacun est tenu de répondre à tous les sondages de Statistique Canada. La *Loi sur la statistique* prévoit des amendes pour ceux qui refusent de s'y prêter, mais Statistique Canada n'a pas la réputation d'être sévère à ce chapitre. C'est en 1952 que les sondages ont débuté. La participation est devenue optionnelle en 1984 pour redevenir obligatoire en 1996 lorsque le taux de réponse a chuté à 74 pour cent et que ce pourcentage a été jugé trop bas par Statistique Canada.

Le questionnaire de 1996 a été envoyé à 16 000 foyers à travers le pays, en proportion à la population. Déjà très long, le questionnaire pourrait être encore plus fastidieux pour ceux ayant des revenus plus élevés s'ils ont une gamme de dépenses et des finances plus complexes. Les questions qu'on y retrouve sont réparties dans les catégories suivantes :

- le logement, l'équipement, les meubles et les services
- l'alimentation, les boissons alcoolisées et les repas au restaurant
- les vêtements
- les produits et services personnels
- les produits et services dentaires et médicaux
- les véhicules et les dépenses afférentes
- les articles et les dépenses ayant trait aux loisirs
- le revenu personnel et les investissements

Le questionnaire est des plus détaillés : les articles de maison comprennent des achats tels les draps et taies d'oreillers, les sacs à poubelle en plastique; les soins pour la santé incluent les trousses de premiers soins, les pansements, les condoms, les seringues, etc., les rasoirs et lames de rasoirs. Dans la section des vêtements féminins, on retrouve la "lingerie"; les dépenses associées aux loisirs incluent "les pellicules photo, le traitement de celles-ci, les épreuves supplémentaires et les agrandissements"; les lectures comprennent les livres en format de

Ce sondage sur les dépenses familiales se démarque des nombreux autres du ministère par sa longueur, soit presque trois heures, par le détail (39 pages) et par l'endroit où il est rempli, soit le domicile même des répondants. Il se penche sur les habitudes de dépenses des ménages et recueille des renseignements sur le revenu, les biens, les dettes, l'occupation et l'éducation.

Un plaignant a qualifié le sondage de "brutalement envahissant" et a mis en doute l'obligation d'y répondre afin de satisfaire aux exigences de Statistique Canada. En outre, il a remarqué que les détails abordés se situaient bien au-delà de ce qui est nécessaire pour l'établissement de l'indice des prix à la consommation. Deux questions en particulier avaient trait aux produits hygiéniques et à l'incontinence et ainsi qu'à l'utilisation de condoms, de seringues, etc. (L'utilisation de ces produits à titre d'exemple est certes un malheureux choix mais voulait simplement illustrer les types de dépenses classées dans leurs catégories respectives).

Selon le plaignant, l'utilisation d'une loi pour forcer une personne à fournir des renseignements, puis à diffuser ceux-ci au profit des entreprises pour l'essor de leurs marchés constituait un conflit d'intérêt et un abus de pouvoir flagrants.

Certains renseignements sont utilisés par Statistique Canada pour mettre à jour l'indice des prix à la consommation, qui est un panier constitué de quelque 600 biens et services dont le suivi permet de mesurer l'inflation. Les données peuvent servir à modifier les articles du panier ou leur poids respectif par rapport au coût total. Elles peuvent aussi servir au gouvernement à classer les dépenses personnelles selon l'âge, la taille de la famille et les revenus. Ces facteurs influencent la politique sur la réforme du bien-être social, les ententes salariales et les paiements de support. Les résultats aident également le gouvernement à comparer le coût de la vie et le niveau de vie des diverses régions et du Canada par rapport aux autres pays.

Il est certain que l'information recueillie est vendue. Dans ses dépliants à l'intention des entreprises, Statistique Canada vante sa capacité à adapter les données du sondage aux besoins particuliers. Certes les données ne sont pas personnelles, mais elles peuvent être associées au revenu familial, à la région métropolitaine, au type d'habitation achetée

La mention "Protégé" accompagnait-elle les demandes faites aux ministères fédéraux ? Les renseignements personnels détenus par le gouvernement fédéral doivent porter la mention "Protégé" pour en prévenir l'ouverture ou l'accès non autorisés. Les requêtes à Santé Canada et aux Archives nationales ne portaient pas cette mention.

Pourquoi souhaitez-vous connaître le motif de départ ? Si l'employé travaillait pour le gouvernement, IDRHC peut procéder au remboursement de la dette en prélevant le montant sur une indemnité de départ, le paiement de congés inutilisés ou encore des paiements de retraite.

Les agents de recouvrement sont-ils autorisés à exiger ces renseignements ? La Commission d'assurance-emploi peut déléguer ses pouvoirs à toute personne ou membre d'un groupe ou de corps. Les délégués comprennent "l'agent de recouvrement, recouvrements des paiements en trop". Les agents de recouvrement sont donc autorisés à recueillir ces renseignements.

Dans une note de service en date de décembre 1997, le chef des services de recouvrement du ministère a traité trois de ces quatre problèmes. Il rappelait au personnel de remettre personnellement les lettres, ou encore par service de livraison confirmé, de ne pas demander le nom de la personne désignée en cas d'urgence sans y être autorisé par un juge et d'utiliser la référence juridique exacte. Actuellement, le personnel de DRHC revoit les lettres afin d'en uniformiser l'énoncé pour éviter que la situation ne se reproduise. La mention "Protégé" sera ajoutée afin de prévenir les divulgations inutiles.

Le Commissaire sait gré au ministère d'avoir donné suite rapidement à ses recommandations.

Sondage de trois heures sur les dépenses familiales : optionnel la prochaine fois

Les sondages de Statistique Canada provoquent souvent des frustrations, surtout ceux traitant des finances personnelles. Cette année, la décision de Statistique Canada de rendre obligatoire une de ses enquêtes régulières a rapidement suscité trois plaintes au Commissariat en plus d'être l'objet d'une attention soutenue de la population de la Colombie-Britannique (mais peu ailleurs).

Après avoir étudié tous les renseignements et les allégations, l'enquêteur a approfondi six aspects du cas. Une allégation à l'effet que les demandes étaient expédiées par télécopieur s'est révélée fausse.

La procédure recommandée pour la cueillette de l'information a-t-elle été suivie par DRHC? La *Loi sur l'assurance-emploi* exige que les agents de recouvrement sollicitent des renseignements de toute personne par un avis signifié à la personne ou encore par un service de livraison confirmé. Cela établit que toute personne, employeur ou institution financière a bel et bien été saisi de l'avis. Il est évident que DRHC n'a pas respecté la procédure parce qu'elle coûtait plus chère et était plus exigeante que la poste régulière.

DRHC peut-il demander les noms et adresses des personnes désignées en cas d'urgence? Le ministère sollicitait des renseignements au sujet de personnes non désignées nommément, soit des renseignements recueillis dans un but précis et limité concernant des personnes qui n'ont rien à voir avec le cas. La *Loi sur l'assurance-emploi* précise que le DRHC ne peut exiger d'un tiers des renseignements sur des personnes non identifiées sans l'autorisation préalable d'un juge. Celle-ci n'avait pas été obtenue.

DRHC peut-il obtenir des institutions financières des renseignements financiers détaillés de clients ? La *Loi sur l'assurance-emploi* autorise à recueillir des renseignements de toute personne, En étant au fait de la situation financière des personnes, DRHC peut en dernier recours saisir les actifs financiers arrivant à échéance. En connaissant les soldes de compte et d'autres biens à court terme, DRHC peut établir un échéancier de remboursement ou encore déterminer le montant qui pourrait être saisi de la paye de ses clients (une fois retracés) sans trop leur nuire. Il semble que certaines institutions financières, qui communiquaient auparavant régulièrement des renseignements sollicités par la poste, s'interrogent maintenant sur les demandes de renseignements financiers provenant de DRHC.

Le personnel de recouvrement a-t-il cité la disposition

habilitante de la loi ? Certaines lettres citaient de façon incorrecte le paragraphe 126 (15) de la *Loi sur l'assurance-emploi*. Ce paragraphe traite des personnes non identifiées et exige l'autorisation d'un juge. La citation exacte est le paragraphe 126 (14).

DRHC resserre son processus de collecte suite à une plainte déposée au Commissariat

Un gestionnaire d'un gouvernement provincial a signalé au Commissariat une collecte d'information menée au fédéral par DRHC qui l'inquiétait. Il avait en effet reçu plus d'une douzaine de demandes de renseignements d'agents de recouvrement de DRHC concernant d'anciens employés de son ministère et il s'interrogeait sur les méthodes de recherche utilisées, la quantité de détails visés et son obligation d'y répondre.

Par la suite, deux autres ministères fédéraux, soit Santé Canada et les Archives nationales, ont eux aussi reçu de semblables demandes et ont communiqué au Commissariat leurs inquiétudes. À la lumière des conclusions de l'enquêteur, ces deux cas ne représenteraient que la pointe de l'iceberg. Lorsqu'il a disposé d'assez de renseignements, le Commissaire a déposé sa propre plainte.

Les agents de recouvrement du DRHC tentent de recueillir les paiements en trop versés par l'Assurance-emploi (AE). Dans environ 80 pour cent des cas, il s'agit de fraude et certains cas visent des sommes importantes. La *Loi sur l'assurance-chômage* prévoit que le ministère dispose de six ans pour recouvrer ces paiements en trop.

Les renseignements recherchés par DRHC variaient d'une ville à une autre, mais la plupart avaient trait à la durée de l'emploi de la personne, le motif de son départ, son adresse domiciliaire et son numéro de téléphone, l'adresse de son institution financière ainsi que le nom et l'adresse de son employeur actuel s'ils sont connus. Les responsables du DRHC à Winnipeg et Moncton demandaient également le nom et l'adresse de la personne désignée par l'ancien employé en cas d'urgence.

Le gestionnaire provincial avait également reçu une demande d'information détaillée concernant les comptes de banque et les soldes d'une personne, ses REER, ses CPG, ses dépôts à terme, ses comptes à d'autres succursales ainsi que tout autre compte d'entreprise. Il était évident qu'il s'agissait là d'une erreur puisqu'un employeur n'aurait pas été en mesure d'avoir de tels renseignements. La requête aurait du être faite à l'institution financière de l'employé et non à son employeur.

Le conjoint de la dame a formellement nié avoir accédé à ce dossier en dredi-la au moment où l'appel avait été effectué. Les entrevues menées par l'enquêteur avec le personnel de la section a permis d'établir que l'ordinateur du mari n'était pas l'un des trois ayant accès aux dossiers de crédit, que personne ne l'avait vu à l'un des terminaux ni demandé à une tierce personne d'effectuer un contrôle en ligne. Cependant, les instructions pour mener une requête en ligne étaient accessibles dans les corbeilles d'entrée des employés. Une requête auprès des Services gouvernementaux de télécommunications et d'informatique téléphonique du gouvernement en vue d'établir avec précision sur quelle ligne l'appel avait été fait n'a donné aucun résultat puisque les registres relèvent seulement les appels interurbains et nullement les appels locaux.

Cette histoire est une première pour ce ministère où tous les ordinaires sont dotés de directives invitant au respect de la vie privée. Le service a réagi en menant sa propre enquête interne et a resserré ses procédures d'accès au système de vérification de crédit. On a changé le code d'accès, assigné des mots de passe individuels à chaque employé afin que chaque contrôle en ligne identifie l'appelant, et l'on a enfin restreint la disponibilité des instructions d'accès. En outre, on a réaffecté l'employé ailleurs.

Le Commissaire a conclu qu'il ne doutait pas qu'on avait bien accédé au dossier de crédit de la dame et a jugé que la plainte était fondée. Bien qu'aucun remède ne puisse être apporté dans le cas présent, des mesures de sécurité plus rigoureuses devraient contribuer à prévenir une récidence. Le Commissaire invite instamment les autres sections affectées à la sécurité à tirer profit de cette expérience.

(Quoique notre bureau identifie automatiquement les ministères contre lesquels des plaintes ont été déposées, le cas présent mènerait à l'identification des personnes concernées et constituerait un bris de l'obligation juridique du Commissaire d'enquêter en privé.)

Un employé accède au dossier d'une dame

On est toujours étonné d'apprendre que les services gouvernementaux fédéraux ont accès aux dossiers de crédit des particuliers. L'explication en est toute simple : beaucoup de postes au sein du gouvernement ont des exigences sécuritaires allant de la plus faible à une exigence de vérification approfondie de la fiabilité pour les activités hautement délicates du renseignement.

Les employeurs procèdent aux vérifications des références de crédit des employés pour s'assurer que les finances de ces derniers ne sont pas dans un état si périlleux qu'ils pourraient être à la merci d'incitatifs financiers ou encore de chantage. Toutefois, en vue de prévenir les abus, seule une poignée d'employés des ministères peuvent accéder aux dossiers de crédit des employés et, en général, il s'agit d'employés affectés aux enquêtes de sécurité.

Cet accès contrôle a déclenché l'alarme lorsqu'une dame s'est plainte du fait qu'une personne, à un ministère où elle n'avait ni travaillé ni recherché un emploi, avait accédé à son dossier au bureau de crédit d'Ottawa. La plainte écrite de la dame incluait une copie de son dossier de crédit qui énumérait les organismes qui y avaient eu accès et comprenait le numéro de téléphone du ministère ainsi que l'identification "Service de sécurité". La dame était en instance de divorce et craignait que son ex-conjoint à l'emploi des services de sécurité ne se soit informé de son dossier de crédit.

Même si l'enquêteur a été en mesure d'établir que le dossier de la dame avait bien été consulté tant au bureau de crédit qu'au service de sécurité du ministère, il lui a été impossible de déterminer par qui. Trois employés sont affectés aux vérifications de crédit à ce ministère à l'aide d'ordinateurs munis d'un modem et utilisant trois numéros de téléphone. Le même mot de passe donne accès à trois ordinateurs programmés pour traiter automatiquement ces requêtes en ligne. (Les demandes téléphoniques exigent le nom de l'appelant afin de l'enregistrer au bureau). Au cours d'une enquête interne, une copie du dossier de crédit de la dame a été trouvée sur support papier par le personnel de la sécurité dans le bureau de son époux, mais sous un format différent des requêtes en ligne.

Le couple avait fourni une preuve de leur citoyenneté canadienne et de leur occupation, mais refusait de communiquer des documents fiscaux. Le ministère désirait s'assurer avant d'émettre un visa que la visiteuse regagnerait bien son pays et ne serait pas un fardeau potentiel pour le Canada. Les documents visaient à établir que les hôtes pouvaient effectivement assumer le coût du séjour de la visiteuse.

Il semble qu'il revient à chaque haut-commissariat de juger, selon les circonstances locales, quels documents sont nécessaires aux requérants. Le Haut-commissariat du Canada à Colombo a commencé à exiger en mars 1997 un avis de cotisation de Revenu Canada afin d'établir la situation financière des hôtes. Il soutenait que les relevés bancaires et les lettres de confirmation d'emploi sont souvent inexacts et difficilement vérifiables. Les affidavits ne peuvent tout simplement pas être appliqués. L'avis de cotisation officiel ne nécessitait pas d'autres vérifications. Puisqu'il établissait le revenu du contribuable et les impôts versés.

Toutefois, même si les documents fiscaux peuvent activer le processus, ils ne sont pas essentiels au traitement des demandes de visa. Les représentants du Haut-commissariat ont reconnu que la communication de renseignements fiscaux est tout à fait volontaire et ils l'ont signalé à tout le personnel. À la demande du Commissariat, ils ont aussi modifié le formulaire de demande afin de supprimer l'énoncé qui précisait que ces renseignements étaient obligatoires.

L'enquêteur a demandé au ministère d'examiner les formulaires de demandes de visa des autres ambassades et hauts-commissariats. Sur un total de 61 réponses, cinq ambassades ou hauts-commissariats stipulaient que les renseignements fiscaux étaient obligatoires. Le ministère a accepté de communiquer avec chacun d'eux et de voir à ce que les formulaires soient modifiés.

Peut-on vraiment évaluer la situation financière de quelqu'un en se basant sur son revenu brut alors qu'on sait que certaines familles vivent très à l'aise avec 60 000 \$ et que d'autres ont de la peine à joindre les deux bouts en disposant de 100 000 \$? La plainte a été jugée fondée et résolue.

la *Loi* devrait comporter une disposition semblable. Celle-ci prévoit que nous fassions le travail qui nous est assigné; les ministères doivent répondre dans des délais raisonnables, et notre bureau doit enquêter sur les plaintes subséquentes.

Le Commissaire ne tolérera pas que des ministères fassent obstruction à ses enquêtes.

Le nombre de cas encore actifs à la fin de l'année atteignait 1780, une augmentation par rapport aux 1147 de la fin de l'année précédente. Une seule question a généré 956 de ces plaintes; il s'agit des plaintes déposées concernant le couplage des données du formulaire de déclaration des Douanes au fichier de l'Assurance-emploi. Le cas est actuellement devant la cour (voir page 99 pour plus d'informations).

Des enquêtes qui traitent contribuent aussi à désillusionner les plaignants lorsque le Commissaire conclut finalement que le ministère concerné n'a pas enfreint leurs droits à la vie privée. Certains concluent que nous ne leur avons pas été d'un grand secours. Toutefois, le pourcentage de plaintes jugées fondées est relativement élevé, soit 48 pour cent si on le compare à la moyenne de une sur trois des ombudsmen.

Les cas décrits ci-dessous illustrent bien le genre d'inquiétudes que les Canadiens portent à l'attention du Commissaire.

Pour l'obtention d'un visa, les hôtes ne sont pas tenus de produire des documents fiscaux

Un couple d'Ottawa a déposé une plainte lorsqu'un journaliste s'est interrogé sur la pratique de Citoyenneté et Immigration d'exiger des renseignements fiscaux auprès d'hôtes canadiens avant d'émettre un visa à leurs visiteurs. La soeur du mari prévoyait se rendre en voyage d'affaires aux États-Unis et désirait passer une semaine avec son frère au Canada.

Le Haut-commissariat du Canada à Colombo, au Sri Lanka a refusé de traiter sa demande de visa, à moins que n'y soit joint un document fiscal confirmant le revenu de l'hôte et de son épouse pour les trois dernières années. Ces documents fiscaux réclamés étaient déclarés obligatoires. On lui a également demandé qui allait défrayer le coût de son voyage au Canada.

Le nombre de plaintes enregistrées continue de grimper et a atteint 2455, par rapport aux 2235 plaintes reçues l'année dernière. Cette hausse s'inscrit dans la hausse moyenne pour les dix dernières années. Au total, 1821 enquêtes ont été complétées, soit environ 900 de moins que l'année précédente. Le chiffre record de l'année dernière était directement lié aux efforts du Commissariat pour éponger l'arrière de plaintes en simplifiant le processus, en mettant en oeuvre un système de traitement accéléré pour certaines plaintes et en utilisant des ressources provenant d'autres sections du bureau. Ces mêmes ressources n'étaient plus à notre disposition cette année.

Au cours des dernières années, le bureau a repensé, puis beaucoup remodelé son processus d'enquête pour éliminer les engorgements et l'accélérer. Mais nous devons faire plus que simplement repenser notre approche. Dès que nous tentons de nouvelles choses, nous sommes déjà dépassés. Le degré de sophistication de notre clientèle augmente ainsi que la complexité des plaintes. Avec la hausse de nouveaux cas, nos enquêteurs sont confrontés à des charges de travail excessives, exigeantes en temps et pratiquement ingérables. La résolution des plaintes est donc retardée et nos enquêteurs s'épuisent.

En plus de charges de travail ingérables, les enquêteurs doivent composer avec le personnel des ministères affecté à la vie privée qui est lui aussi surchargé de travail, impatient et non coopératif. Frustré par les demandes répétées de requérants qui se servent de la *Loi sur la protection des renseignements personnels* à titre d'outil personnel de représailles contre des ministères cibles, le personnel de fait se dérobe aux enquêteurs en remettant ou reportant des réunions, en retardant l'identification des contacts à l'intérieur des ministères ou encore en ne produisant pas les dossiers que les enquêteurs doivent étudier.

Le Commissariat comprend la problématique vécue par les ministères, en déposant des demandes répétées, certains requérants abusent presque du système. Ils déposent également des plaintes à répétition. Malgré cela, la *Loi* ne prévoit pas de disposition autorisant les ministères ou le Commissaire à ignorer ou reporter les demandes répétées ou les plaintes frivoles ou irritantes. D'ailleurs le Commissaire ne juge pas que

compréhensible, c'est néanmoins un premier pas vers la perte de l'autonomie. C'est une chose que de prendre des décisions éclairées en matière de santé, c'en est une autre que d'y être forcé.

Ébauche de code de l'Association médicale canadienne

Un autre signe encourageant est le code de protection de la vie privée sur la santé, qui en est à l'étape finale de son élaboration. L'ébauche de code du 16 juin, qui est exhaustif, dépasse ce que nous proposons dans notre rapport annuel de l'an dernier. En quoi le dépasse-t-il ? Alors que les grandes lignes du code de l'Association médicale canadienne (AMC) respectent le code type proposé par l'Association canadienne de normalisation, son contenu s'inspire du rapport du comité parlementaire intitulé *La vie privée : où se situe la frontière?* Ce document, on s'en souviendra, reconnaît la vie privée comme un droit de la personne et comme valeur sociale.

Dans son document de travail, l'AMC reconnaît que les initiatives signalées à la rubrique « protection de vie privée » ont souvent moins à faire avec la protection de la vie privée que l'accès à une fin secondaire; elle reconnaît que si l'autorisation ne revient pas aux patients, on parle à double sens si l'on soutient qu'en accordant l'accès seulement aux personnes autorisées, on protège le droit à la vie privée. Ce qui incite l'AMC à promouvoir la vie privée, c'est bien sûr de protéger l'intégrité de la relation médecin-patient. En prononçant le serment d'Hippocrate, le médecin s'engage à « taire, quoi qu'il voit ou entende dans la société pendant l'exercice ou même hors de l'exercice de sa profession, ce qui ne doit jamais être divulgué, le regardant comme un secret ». Comme le document de travail de l'AMC le souligne, en raison de la haute confiance qu'on place dans le médecin et de la notion de confidentialité, le médecin pourrait devenir un instrument de trahison malgré lui. On trouve, à l'affût derrière lui, un grand nombre d'autres d'utilisateurs que ne préoccupent en rien la relation patient-médecin, mais qui sont anxieux d'avoir accès aux renseignements recueillis par le médecin.

Le Code sera présenté au Comité exécutif de l'AMC en séance plénière au mois de septembre.

compromettrait pas la vie privée des patients. Toutefois, les partisans du réseau national d'information sur la santé ont soutenu qu'une bonne sécurité constitue la vraie protection de la vie privée. Ils ont insisté pour que le réseau soit d'abord mis en place, puis qu'on s'occupe après coup de corriger les lacunes en matière de vie privée.

(Au moment d'aller sous presse, les délibérations de l'assemblée n'avaient pas été rendues publiques, et aucun plan d'action n'avait été annoncé.)

Il faut rappeler aux concepteurs du réseau que l'utilisation de renseignements médicaux sans le consentement de l'intéressé(e) constitue une intrusion dans la vie privée, quel que soit le système de sécurité utilisé. C'est là que réside toute la différence entre assurer la sécurité et préserver la vie privée, et c'est ce qu'il faut maintenir à tout prix.

Les renseignements médicaux et les circonstances dans lesquelles ils sont confiés sont uniques. Lorsque nous sommes malades ou blessés, nous sommes de véritables otages. Vulnérables et désireux de recouvrer la santé, nous ressentons le besoin de confier des détails intimes de notre vie que, dans d'autres circonstances, nous garderions pour nous. Certes, en cas d'urgence, le personnel soignant a besoin de tous les renseignements personnels qui peuvent aider. Une fois enregistrés, ces renseignements intimes pourraient électriquement nous suivre du berceau à la tombe.

À ce point, le patient (et aussi le médecin, pourait-on soutenir) n'a plus le contrôle. Les détails pourraient dépasser largement la relation de confiance établie entre le patient et le médecin. Ces renseignements confiés volontairement en vue d'obtenir un traitement médical pourraient être diffusés à un régime de santé élargi, voir parvenir à un employeur, actuel ou éventuel, à une compagnie d'assurance ou à un bureau de crédit. Ils pourraient servir à des fins non prévues, avec des conséquences désastreuses.

Un régime public de soins de la santé semble justifier des intrusions plus grandes dans la vie privée. À mesure que les liens se précisent entre le mode de vie, la pauvreté et la santé, on sera de plus en plus tenté de suivre, d'évaluer et enfin d'influencer nos choix afin que nous ne devenions pas un fardeau pour le régime. Quoique cela soit

Protection des renseignements personnels dans le domaine de la santé - bilan pas très reluisant

Dans notre rapport annuel de l'an dernier, nous expliquions les risques associés au projet de stratégie nationale sur la santé, qui consiste en un réseau national d'information dans le domaine de la santé. Il semble que nous ayons touché là une corde sensible.

Ceux qui sont vivement en faveur d'un tel réseau sont ceux qui souhaitent avoir accès aux dossiers médicaux confidentiels afin de rationaliser les dépenses en soins de la santé, d'accroître la fluidité des échanges d'information entre les administrations et de recueillir des données probantes sur les facteurs influant sur la santé des Canadiens. Ce sont là des objectifs fort louables. Toutefois, les dossiers médicaux en ligne (couplés aux données socio-économiques permettant d'établir le profil des patients) pourraient transformer les soins de santé en véritable cirque.

Mais heureusement, il semble que d'autres personnes soient à l'écoute. Ainsi, en février dernier, des représentants du gouvernement, des professionnels de la santé, du milieu de l'enseignement, des organisations de consommateurs et du monde des affaires se sont réunis lors de la Conférence nationale sur l'info-structure de la santé et ont élaboré une stratégie sur l'établissement d'une telle info-structure. On remarquait en tête des sujets abordés le thème *Vie privée, sécurité et confidentialité*.

Dans son discours d'ouverture, le ministre de la Santé de l'époque, Allan Rock, a parlé de la vie privée comme étant peut-être "la question la plus importante. Pour qu'une stratégie nationale soit crédible, il faut que le public soit convaincu que la vie privée demeurera protégée". Le ministre a reconnu que beaucoup de personnes, dans le domaine de la santé, s'inquiètent de ne pas pouvoir accéder aux renseignements dont ils ont besoin si des mesures rigoureuses de protection de la vie privée sont adoptées. Cependant, il s'est dit déterminé à faire en sorte que les renseignements personnels les plus délicats des Canadiens soient protégés adéquatement.

Au cours de la séance de travail, d'autres personnes se sont déclarées en faveur d'un régime de soins de santé efficace et utile qui ne

au processus de résolution des plaintes du Commissaire, elle devrait avoir le droit de le faire. Chacune des étapes du processus de résolution devrait avoir des délais fixes afin d'éviter les retards inacceptables.

Au besoin, le Commissaire émettra des recommandations au sujet de la collecte, de la conservation, de l'utilisation ou la communication de renseignements personnels, ainsi qu'en ce qui a trait à tout refus d'accès ou de correction. En outre, il devrait avoir le droit de proposer tout recours qu'il juge approprié pour le plaignant. Le Commissariat devrait être autorisé à enquêter sur les plaintes et à les résoudre, comme c'est actuellement le cas en vertu de la *Loi sur la protection des renseignements personnels*.

Les parties devraient être tenues de participer au processus de médiation mis en oeuvre par le Commissariat. Le Commissaire soumettrait alors une évaluation non-obligatoire des positions individuelles des parties.

Vérification de conformité

La loi devrait exiger que les organisations se soumettent à des vérifications périodiques de leurs pratiques de gestion de l'information. Elles auraient la possibilité de nommer un vérificateur de leur choix et elles devraient rectifier la situation dans un laps de temps raisonnable suite aux recommandations provenant de la vérification. En outre, la loi autoriserait le Commissaire à mener des vérifications auprès d'une ou plusieurs organisations s'il a des motifs raisonnables de soupçonner que leurs pratiques en matière d'information laissent à désirer ou encore s'il a reçu de nombreuses plaintes similaires.

Évaluation de l'impact sur la vie privée

Le Commissaire devrait fournir aux organisations les outils leur permettant d'évaluer l'impact de toutes leurs activités sur la vie privée. En s'assurant dès le départ de la mise en oeuvre, dans leurs activités, de pratiques de gestion de l'information équitables, les organisations pourraient réaliser de grosses économies en n'ayant pas à reprendre la phase initiale de conception. Par ailleurs, le Commissaire devrait avoir le droit de surveiller les communications effectuées aux fins de recherches et de statistiques.

Le Commissaire devrait également avoir l'autorisation expresse de relever et d'évaluer les questions qui peuvent affecter la vie privée, par exemple, la surveillance en milieu de travail, les technologies personnelles d'identification et le suivi de renseignements pertinents aux achats, même si ces questions n'ont pas généré de plainte. Doté d'une infrastructure et de ressources adéquates, le bureau du Commissaire pourrait devenir un organisme de surveillance efficace.

L'élargissement de la compétence du Commissaire à la protection de la vie privée au secteur privé sous réglementation fédérale serait conforme à la portée des autres organismes de surveillance fédéraux tel le bureau du Commissaire aux langues officielles.

Certains secteurs commerciaux ont suggéré que ce mécanisme serait acceptable s'il était géré par des organismes de réglementation déjà en place comme le surintendant des institutions financières dans le secteur bancaire. Cependant cela pourrait aboutir à l'existence de plusieurs organismes de réglementation inexpérimentés dans le domaine de la protection des données nominatives et se terminerait inamiquablement par une application et une observation variables des normes en matière de vie privée.

Eduquer le public

Aucune loi n'est efficace si le public et les entreprises ne la comprennent pas. Les organisations et leurs associations respectives devraient porter la responsabilité première d'éduquer leurs employés, leurs cadres et le public. Des consommateurs et des employés avertis sont plus susceptibles d'encourager les organisations à adopter des pratiques équitables en matière d'information. Cependant la loi proposée devrait précisément mandater le Commissaire et le doter des ressources nécessaires pour accroître la sensibilisation aux nouvelles questions et technologies susceptibles d'affecter la vie privée.

Processus des plaintes

Du point de vue administratif, le processus des plaintes doit être simple pour le plaignant et l'entreprise qui détiennent les renseignements personnels. Une personne devrait commencer par tenter de résoudre ses plaintes directement avec l'organisation concernée. Puisque les plaintes proviennent souvent de malentendus, beaucoup peuvent être résolues à cette étape. Cependant, si l'organisation préfère s'en remettre

Il est certain que les codes sectoriels aident à guider efficacement les entreprises privées, mais ils ne devraient pas faire partie intégrante du cadre législatif proposé parce qu'ils sont peu pratiques. En premier lieu, il serait difficile de définir des secteurs puisque les industries continuent de converger et de se réaligner. Il serait également difficile d'assurer que les codes régissant chacune des entreprises individuelles d'un secteur soient conformes à la norme sectorielle. Enfin, les codes sectoriels pourraient être inutiles. La loi du Québec sur les données nominatives dans le secteur privé, en vigueur depuis janvier 1994, ne recourt pas aux codes sectoriels, ce qui n'a pas été préjudiciable.

Une autre caractéristique de certaines lois nationales veut que les entreprises privées inscrivent leurs bases de données nominatives auprès d'une autorité centrale. L'inscription serait un exercice inutilement coûteux et bureaucratique qui monopoliserait à mauvais escient des ressources, lesquelles pourraient être mieux utilisées à défendre les intérêts relatifs à la vie privée.

Droit de regard

Quelques que soient ses caractéristiques, la loi devra comporter un mécanisme de surveillance indépendant; bref, un organisme qui examinera la conformité et résoudra les conflits. Il existe diverses options : le recours aux tribunaux pour les plaignants — processus coûteux et lourd pour toutes les parties (y compris les tribunaux) — la création de tribunaux quasi judiciaires, l'établissement de commissaires aux données pouvant des ordonnances.

Le modèle de l'ombudsman en place en vertu de la *Loi sur la protection des renseignements personnels* est l'approche la plus efficace. Un ombudsman assure l'équité administrative en s'appuyant sur les connaissances, l'impartialité et des pouvoirs d'enquêtes importants. Pour que le mécanisme de surveillance soit efficace, il faut qu'il appuie au maximum la consultation, la conciliation et la négociation, en recourant à la contrainte et à la compulsion le moins possible. La possibilité de mauvaise presse demeure la houllette de l'ombudsman et s'avère un outil efficace s'il est utilisé judicieusement.

Le droit de regard du Commissaire à la protection de la vie privée comprendrait la promotion de pratiques équitables en matière d'information, la résolution des plaintes et la conduite de vérifications.

des lois du Canada et du code type de protection des renseignements personnels de l'Association canadienne de normalisation.

La protection des renseignements personnels peut aussi être perçue comme une question relevant du gouvernement fédéral en vertu de la rubrique de la Constitution relative aux traités et accords commerciaux. Cette interprétation de la Constitution permettrait au gouvernement fédéral de réglementer la protection des renseignements personnels dans tout le secteur privé.

Le code de la CSA

Le document de travail souligne le travail de l'Association canadienne de normalisation (CSA) qui a rassemblé pour l'ébauche du code type des représentants du secteur public, du monde des affaires, des consommateurs et des syndicats. Le code établit des principes pour la collecte, l'utilisation, la communication et la protection des données personnelles tout en garantissant aux particuliers l'accès et le droit de faire rectifier leurs renseignements le cas échéant. L'Association canadienne de normalisation a depuis adopté le code à titre de norme nationale en 1996.

Appliqués avec rigueur, les principes élargis de ce code constituent une assise solide pour la création d'une loi sur la vie privée. En outre, le code a l'avantage d'être approuvé par plusieurs commissaires provinciaux à la vie privée. Cependant, il comporte des lacunes qui donneraient lieu à une réglementation normalisée des données qui ne serait pas suffisamment rigoureuse et conférerait seulement l'illusion d'une protection efficace des renseignements personnels.

L'élaboration d'une nouvelle loi sur la vie privée soulève plusieurs questions quant à son administration et la surveillance qu'elle permettrait d'exercer. Afin qu'elle fonctionne réellement, cette loi ne doit pas être encombrante ni bureaucratique, et son processus de responsabilisation ne doit pas se révéler épuisant pour les consommateurs. Le document aborde plusieurs options possibles.

Codes sectoriels et enregistrement

Alors que des pays exigent ou incitent les secteurs de l'industrie à élaborer des codes plus précis, adaptés aux exigences de l'industrie et des clients, nous n'encourageons pas le concept de codes dans le régime de réglementation canadien.

et traite des options de mise en oeuvre de la loi et d'un mécanisme de suivi. Le document vise moins à assurer la protection des renseignements personnels qu'à susciter la confiance de s'engager dans le commerce électronique. Il est révélateur que la citation d'introduction du document lui-même dans le discours du trône de septembre 1997 ne fasse nullement référence à la vie privée ou aux données nominatives.

Une loi permettant au gouvernement fédéral de régir la protection de la vie privée dans le secteur privé est importante pour plusieurs raisons. La distinction entre les secteurs privé et public s'estompe. De plus en plus, le gouvernement général, à l'instar de nombre d'autres gouvernements, privatise, commercialise et confie à l'extérieur les fonctions gouvernementales. Dans certains cas, on a retranché des données nominatives de la *Loi sur la protection des renseignements personnels*. En outre, l'évolution de la technologie a fait monter les enjeux dans les relations entre les Canadiens, le secteur privé et le gouvernement et a permis la collecte, l'utilisation et la communication des renseignements personnels à une échelle sans précédent.

Une protection légale des renseignements personnels dans le secteur privé sous réglementation fédérale est un objectif désormais réalisable. La solution par excellence serait bien sûr que les provinces et les territoires disposant de lois uniformes régissant la vie privée et les données nominatives. Le Québec a déjà mis en oeuvre une semblable loi : il est en fait la seule administration nord-américaine à l'avoir fait.

Règles du jeu égales

Le document de travail préconise l'harmonisation des lois régissant la vie privée et les données nominatives dans toutes les administrations canadiennes. Cela est essentiel pour que les règles du jeu soient équitables à l'échelle du pays et si nous souhaitons éviter que certaines administrations deviennent de véritables paradis pour les manipulateurs de données, où des lois moins exigeantes seraient susceptibles d'attirer certaines entreprises désireuses de se soustraire à leurs obligations en matière de vie privée. Des lois provinciales applicables au secteur privé devraient s'inspirer des meilleurs éléments de la loi fédérale sur le secteur privé sous réglementation fédérale, de la loi régissant le secteur privé au Québec, du document intitulé *Private Sector Protection of Personal Information Act* publié par la Conférence sur l'uniformisation

- En septembre 1996, le ministre de la Justice et Solliciteur général de l'époque, Allan Rock, annonçait qu'on visait à adopter d'ici l'an 2000, une loi efficace et exécutoire protégeant les droits à la vie privée dans le secteur privé.

- En avril 1997, la Chambre des communes a endossé à l'unanimité une motion émanant du député Paul Crête proposant d'étendre la *Loi sur la protection des renseignements personnels* à toutes les sociétés d'État.

- En avril 1997, le Comité permanent sur les droits de la personne et le statut des personnes handicapées a publié un rapport intitulé *La vie privée : où se situe la frontière?*. Celui-ci proposait qu'on substitue à la *Loi sur la protection des renseignements personnels* une loi sur la protection des données nominatives qui s'appliquerait aux renseignements personnels détenus par le Parlement, les ministères, les organismes, les sociétés d'État, les conseils et commissions ainsi que les entreprises et industries sous réglementation fédérale.

- En mars 1998, la Conférence sur l'uniformisation des lois du Canada, un organisme indépendant et non gouvernemental, a publié sa plus récente ébauche d'une loi uniforme de protection des données nominatives dans le secteur privé.

La proposition gouvernementale : un bon point de départ

Comme la question de la vie privée dans le secteur privé est d'envergure nationale, c'est au gouvernement fédéral à faire preuve de leadership. Heureusement, les principaux secteurs commerciaux (banques, communications, transport) relèvent déjà de la compétence fédérale et comptent parmi les plus importants collecteurs et utilisateurs de renseignements personnels. Aujourd'hui, quinze ans après avoir abordé publiquement pour la première fois l'éventualité de protéger les renseignements personnels dans le secteur privé sous compétence fédérale, le gouvernement se dispose à ébaucher un projet de loi.

Le document de travail d'Industrie Canada et du ministère de la Justice décrit l'état actuel des lois régissant la vie privée au Canada et explique pourquoi cela ne suffit plus à protéger les Canadiens dans le contexte actuel. Il établit les principes de base d'une loi efficace sur la vie privée

Une loi sur la vie privée applicable au secteur privé

Depuis longtemps le besoin se fait sentir beaucoup au Canada d'une loi exhaustive protégeant les renseignements personnels dans le secteur privé. Jusqu'à très récemment, une telle loi, dans le processus législatif, semblait être comme la mariée laissée au pied de l'autel. Mais deux initiatives redonnent espoir.

La première est la publication, en janvier 1998, du document de travail du gouvernement intitulé *La protection des renseignements personnels : Pour une économie et une société de l'information au Canada*. Le document tentait d'abord d'obtenir les commentaires du public sur un modèle de loi pour protéger les renseignements personnels dans le secteur privé sous réglementation fédérale. La seconde initiative est une ébauche de la loi de protection des données nominatives préparée à l'intention de la Conférence sur l'uniformisation des lois du Canada et qui pourrait servir d'armature à une nouvelle législation cohérente s'appliquant à toutes les administrations.

Les tentatives faites pour régler la protection des données nominatives dans le secteur privé remontent aux débuts des années 1980. Lorsque le projet de loi, devenu la *Loi sur la protection des renseignements personnels*, a été soumis à la Chambre en troisième lecture en juin 1982, le ministre des Communications de l'époque avait noté que dans l'élaboration d'une loi sur la vie privée, la prochaine étape consistait à en étendre les principes au secteur privé sous réglementation fédérale. Depuis, la question s'est posée à plusieurs reprises.

- En mars 1987, le Comité permanent sur la justice ainsi que le Solliciteur général s'étaient prononcés en faveur d'une loi régissant le secteur privé dans le rapport intitulé *Une question à deux volets : Comment améliorer le droit d'accès à l'information tout en renforçant les mesures de protection des renseignements personnels*.

- En mai 1996, le ministre fédéral de l'Industrie annonçait la tenue de consultations avec les provinces et les autres parties intéressées afin d'obtenir des propositions pour un cadre législatif s'appliquant à la protection des renseignements personnels dans le secteur privé.

ce dernier pourrait profiter de l'occasion pour établir un régime unique de liens et de subventions avec l'ensemble de ses officiers. Je veux terminer en exprimant publiquement ma profonde gratitude envers un personnel et des collègues dévoués. Tout crédit à ce bureau ou à moi-même leur revient en raison de leur haut degré de professionnalisme. Jamais aucun Commissaire n'a été plus en dette envers son personnel.

aussi dissemblables que les pôles et l'équateur, et n'ont en commun que l'objectif de rendre accessibles au public des renseignements détenus par le gouvernement fédéral. La seconde ne tranche que sur la communication, ou non, d'un document gouvernemental, alors que la première est autrement plus vaste.

L'accès aux documents gouvernementaux est un droit administratif caractéristique des pays ayant récemment accédé à la démocratie, bien que peu de ces États aient de semblables lois. Par contre, le droit à la vie privée est un droit fondamental de chaque personne et qui touche presque tous les aspects de sa vie. Il s'agit, pour reprendre les termes de la Cour suprême du Canada, d'un élément fondamental à la liberté individuelle. Voilà la liberté que notre Commissariat s'acharne à défendre. Nombreuses sont les démocraties modernes qui protègent ce droit et en confient la responsabilité à un arbitre. Il n'y a qu'au Canada, et encore seulement dans les provinces, que cet arbitre cumule la défense de la vie privée et du droit d'accès aux documents gouvernementaux.

La responsabilité de la future loi protégeant la vie privée au sein des entreprises canadiennes pourrait très naturellement échoir à notre Commissariat, nous permettant ainsi de demander le divorce une fois pour toutes. Le secteur privé a besoin de savoir que le législateur n'a qu'une priorité en tête, soit la gestion des renseignements personnels de leurs employés et de leurs clients. Un commissaire distinct ne pourrait donc être accusé de s'intéresser aux dossiers administratifs de ces entreprises.

Il me reste à conclure en recommandant au Parlement de régler un problème imprévu à l'origine, mais qui nous handicape sérieusement. Le Commissariat est en effet orphelin. Bien que le Commissaire à la vie privée soit un officier parlementaire, le Parlement se penche rarement et trop brièvement sur les enjeux dont il traite et sur ses opérations. Le budget du Commissariat fait partie de celui du ministère de la Justice, ce qui m'oblige à quémander des fonds d'un ministre au sujet des agissements duquel la loi pourrait m'obliger à mener enquête. Un tel état de fait indispose tout le monde et compromet mon impartialité. La loi devrait par conséquent établir le rapport direct qui existe entre mon Commissariat et le Parlement, et

cours des années, cependant, le Commissariat a par la force des choses hérité de responsabilités dont la loi ne fait aucune mention, telle l'analyse de politiques et la recherche dont dépendent le Parlement et la population pour se maintenir au fait des grands enjeux en matière de protection de la vie privée. Ce septennat nous a donnés l'examen de l'Internet, des empreintes digitales numériques, de l'analyse de données et du système national de renseignements sur la santé. Sans ces activités que nous accomplissons avec peine faute de ressources et de mandat, notre Commissariat ne serait d'aucune utilité au législateur ni à la population.

Et que dire de la surcharge d'enquêtes dont le nombre a doublé depuis toutes ces années, accablant nos enquêteurs dont l'effectif n'a pour ainsi dire pas changé?

N'oublions pas non plus la soif grandissante de renseignements qui s'est emparée des citoyens inquiets des impacts des technologies, et qui se tournent vers nous pour éclairer leur lanterne. Cela n'est pas non plus dans notre mandat (ni dans notre budget), mais nul n'en avait averti les citoyens. Le Parlement n'avait peut-être pas prévu cet état de fait, mais il n'en reste pas moins que nous ne pouvons au mieux traiter qu'une trop faible partie des innombrables demandes de renseignements que nous avons reçues ces dernières années.

Le Comité de la Chambre des communes sur la justice s'est penché en 1987 sur les problèmes précédents, qui ont de plus été touchés dans le rapport *Vie privée : où se situe la frontière?*, mais en vain. Le ministère de la justice, responsable de la *Loi sur la protection des renseignements personnels*, a cependant récemment étudié certaines modifications à cette dernière, mais la bureaucratie prend parfois bien du temps à atteindre ses objectifs.

Je ne saurais conclure sans soulever un sujet qui m'agace depuis le début de mon septennat, alors que l'on a commencé à vouloir faire croire qu'il y aurait du bon à fusionner les Commissariats à l'information et à la vie privée du Canada. J'ai rongé mon frein à chaque apparition de cette idée, préférant ne m'occuper que de mes affaires et souhaitant que les autres se consacrent davantage aux leurs.

Mais il est désormais temps d'enterrer une telle notion. Les *Loi sur la protection des renseignements personnels* et *Loi sur l'accès à l'information* sont

Il est également urgent de modifier les pouvoirs et le rôle dévolus au Commissariat. L'emphase initiale sur les enquêtes demeure juridiquement prépondérante et la seule qui soit subventionnée. Au

Le temps de faire du ménage

contourne la loi en sous-traitant certains services tels des sondages ou des enquêtes, ou ne décline la responsabilité de certains renseignements telles les notes personnelles prises par les membres de conseils. La loi pêche aussi par son laxisme au chapitre des ententes et accords de partage de renseignements entre le gouvernement fédéral et d'autres gouvernements canadiens ou étrangers. Bien que ces ententes soient essentielles à la bonne gestion publique et fassent généralement l'objet d'une reconnaissance spécifique dans plusieurs lois, dont la *Loi sur la protection des renseignements personnels*, le libellé des plus vagues de cette dernière provoque des abus : il existe des centaines de ces ententes, dont nous ne connaissons qu'une infime partie. Mais le peu que nous en savons nous inquiète, car bon nombre des échanges de renseignements se font à l'insu de la population, ou même du personnel des organismes concernés!

Cette banalisation des échanges ainsi que la quantité des renseignements qui sont visés devraient convaincre les organismes fédéraux de s'assurer que les destinataires protègent adéquatement la confidentialité des renseignements qui leur sont envoyés, ce que la loi pourrait obliger par contrat, lequel permettrait également aux organismes fédéraux de prendre les moyens nécessaires à la vérification de l'application de ces exigences. Un régime comparable devrait par ailleurs viser toute entreprise privée héritant de la responsabilité d'un programme ou d'une activité relevant auparavant du gouvernement fédéral.

Le gouvernement fédéral a partiellement accédé aux lignes précédentes, le Conseil du Trésor ayant ordonné aux ministères de garantir par contrat la protection des renseignements personnels visés par les ententes de privatisation. Tout nouvel organisme demeurant de compétence fédérale sera assujéti à la *Loi sur la protection des renseignements personnels*, et tout organisme devenant de compétence provinciale sera tenu par contrat de vente de protéger les renseignements personnels lui échouant.

technologiques. Ainsi, les échantillons d'ADN (tissus, sang et sperme) devraient tomber sous le coup de cette définition. La loi gagnerait également à préciser les renseignements ayant trait aux responsabilités ou au poste d'un fonctionnaire, ce qui aurait pu éviter certains litiges ruineux ayant porté sur les fiches d'accès en dehors des heures ouvrables ou sur les privilèges de stationnement.

Les dispositions de la loi entourant l'accès par un individu aux renseignements le concernant et celles visant le besoin de son consentement à la divulgation de ces derniers sont assorties de nombreuses exceptions et exclusions qui devraient être revues, bien que la plupart soient justifiées. Il est effectivement illlogique de permettre à une personne faisant l'objet d'une enquête d'obtenir copie des renseignements policiers la concernant, ou à un terroriste de prendre connaissance des dossiers du SCRS à son sujet. Certaines exceptions restent cependant abusives.

L'alinéa 22(1)a) de la loi permet notamment aux organismes fédéraux d'enquête de refuser la communication de tout renseignement relatif à l'administration d'une loi fédérale ou provinciale. Cette disposition est suffisamment vague pour permettre à toutes fins pratiques à neuf organismes fédéraux de refuser la communication de tous les renseignements personnels qu'ils détiennent.

Il me déplait particulièrement de constater que la loi permet à tout ministre fédéral de refuser de communiquer à une personne les renseignements la concernant pour la simple raison que la loi le lui permet, et ce même si la divulgation ne porte aucun préjudice. La loi devrait plutôt exiger d'un organisme fédéral qu'il prouve le préjudice qu'entraînerait la communication avant de la refuser, et cette exigence devrait s'appliquer à chaque exception ou exclusion.

La grande importance des articles 4 à 8 de la loi (visant la collecte, l'utilisation et la communication de renseignements personnels) devrait pousser le Parlement à élargir l'accès aux tribunaux pour tout manquement à ces dispositions, permettant ainsi aux individus lésés d'obtenir des arrêts, ou même des dommages et intérêts si le manquement était de nature délictuelle.

Il faudrait également resserrer la notion de "contrôle" des renseignements personnels, ce qui éviterait qu'un organisme fédéral ne

Effectuant un bref aparté sur le code promoteur de l'Association médicale canadienne, il semble que de tels codes sont possibles lorsque vous, ainsi qu'en témoigne le nouveau code de déontologie de l'Association dentaire canadienne, obligatoire dans certaines provinces. Ce dernier reconnaît à chaque patient le droit à des soins dentaires confidentiels et libres de toute ingérence de tiers. Le patient peut consulter et photocopier son dossier, contrôler la divulgation de ses renseignements, et apprendre les coordonnées des personnes à qui il permettrait d'en prendre connaissance. Tout tiers (tel Revenu Canada ou une compagnie d'assurances) ne peut accéder au dossier d'un patient qu'à des fins de vérification, et qu'après que tous les renseignements superflus ou permettant d'identifier ce dernier en ont été retirés. Les membres de l'Association dentaire canadienne ne pourront que se louer d'une telle initiative, laquelle prouve l'intérêt de leur association pour leurs patients.

Mettre à jour la Loi sur la protection des renseignements personnels : un autre défi pour l'an 2000

Les grands enjeux qui précèdent ont peut-être éclipsé le besoin pourtant criant de mettre à jour la *Loi sur la protection des renseignements personnels*. Cette loi, vieille de 15 ans, régit la gestion des renseignements personnels détenus par un grand nombre d'organismes fédéraux (mais pas tous). À l'époque, c'était une bonne loi dont les grandes lignes ont bien résisté aux années, mais dont l'évolution des enjeux pour notre vie privée a exposé les faiblesses.

La plus grande en est certainement la portée, restreinte aux seuls renseignements personnels. En fait, la vie privée n'est véritablement que bien peu protégée au Canada, peu de provinces considérant ses atteintes comme un délit, et la *Charte canadienne des droits et libertés* (voir la page 102) ne la défendant qu'en dernier recours. En fait, le rapport déposé l'an dernier par le Comité de la Chambre des communes sur les droits de la personne, intitulé *La vie privée : où se situe la frontière?*, apprendra au gouvernement tout ce qu'il souhaite savoir sur la meilleure façon de bien protéger la vie privée de chaque Canadien. Mais revenons à la *Loi sur la protection des renseignements personnels*. Parmi les changements à y apporter, soulevons tout d'abord le besoin d'élargir la définition de "renseignement personnel" afin de refléter les progrès

services. Les derniers soutiennent qu'un profil plus complet de l'état de santé de chaque citoyen permettra de nouvelles avancées médicales, particulièrement en matière de prévention.

Les médecins canadiens, cependant, semblent gravement préoccupés en dépit d'une certaine reconnaissance des avantages que procurera pareil système. En effet, ce dernier pourrait mener à l'érosion, voire à la disparition du principe de base de leur déontologie : l'absolue confidentialité des communications entre un patient et son médecin. L'Association médicale canadienne vient par conséquent d'élaborer un code de protection de la vie privée, dont le principe directeur est l'exigence qu'un patient consente à chacune des divulgations de ses renseignements. Ce code, dont l'ébauche actuelle est réfléchie et détaillée, pourrait donc devenir le serment d'Hippocrate de l'âge de l'information.

Il s'agit là d'un tournant majeur dans la gestion des données médicales, puisque le code force les tenants d'un système national de renseignement sur la santé à élaborer des mécanismes de protection de la vie privée qui recevront l'aval de la communauté médicale.

Le comité consultatif fédéral n'ignore pas cet enjeu, puisque son co-président, le Dr Tom Noseworthy de Calgary, s'est publiquement engagé à ce que le système national protège pleinement la vie privée. Bien qu'une telle promesse ne puisse que recueillir notre appui et celui de nos collègues, il demeure naïf et irréaliste de sous-estimer les difficultés et les complexités administratives et technologiques auxquelles elle se heurtera, notamment en matière d'échanges de renseignements. N'oublions donc pas que le maintien de notre régime public de soins de santé ne devra pas signifier l'abandon de notre droit fondamental à la confidentialité médicale.

Nous nous permettons par conséquent les conseils suivants : consultez et faites intervenir les experts en vie privée, et ce au maximum. Ne faites pas dès le début fausse route, et assurez-vous du soutien de la population (et des commissaires à la vie privée). Sinon, vous échouerez, et votre système national aussi.

Il s'agit là d'un dossier que nous suivons de très près, car nous sommes convaincus qu'un tel projet ne devra pas voir le jour s'il signifie la disparition de nos droits actuels.

Le futur projet de loi devra également surmonter l'obstacle que représente pour certains l'inefficacité pouvant résulter du manque de concertation des deux principaux paliers de gouvernement. La majorité des entreprises privées relèvent effectivement des provinces, et une harmonisation des lois et de l'approche est certes souhaitable. Des normes nationales uniformes faciliteraient les choses pour le monde des affaires et pour le gouvernement, elles seraient compréhensibles pour les individus et elles éviteraient le spectre de paradis des données au sein de la fédération. C'est là l'idéal. Néanmoins, si on ne peut convaincre les autres de protéger les droits des citoyens sur le marché, il faudra que le gouvernement fédéral donne l'exemple; c'est un rôle qu'il semble disposé à assumer. L'attention se porte maintenant sur les provinces qui ont la compétence à l'égard d'une grande partie du secteur privé.

Un Internet médical?

Notre seconde grande préoccupation vise le sort du dossier médical personnel. Aucun autre projet que celui d'un système national de renseignements sur la santé ne concrétise mieux selon nous les dangers qui menacent notre vie privée et la confidentialité de nos renseignements personnels. Un tel système permettra à des hordes de professionnels de la santé, de bureaucrates et de chercheurs d'accéder électroniquement aux dossiers médicaux de presque toute la population canadienne. Sachant la tragédie que peut représenter la divulgation non autorisée de nos renseignements médicaux par une seule personne, comment pourrions-nous désormais faire confiance aux milliers de gens qui verront notre dossier?

L'implantation d'un système national de renseignements de santé n'en progresse pas moins, pilotée par un comité consultatif fédéral dont aucun des membres ne s'y connaît en matière de protection de la vie privée et des renseignements personnels. Il est par ailleurs surprenant de constater le peu de réactions que ce projet a suscité, compte tenu de l'impact majeur qu'il aura sur chacun de nous.

Les tenants de ce projet sont légion, allant des bureaucrates de la santé de tous les paliers de gouvernement (du fédéral au municipal) aux chercheurs. Les premiers escomptent de substantielles économies, une meilleure lutte contre la fraude et une prestation plus efficace des

En 1996, le gouvernement fédéral est parvenu aux mêmes conclusions, poussé également par son désir de faire du Canada le chef de file en

matière de commerce électronique : en effet, aucun Canadien n'ac-

ceptera de transiger électroniquement avec un magasin, une banque ou le ministre du Revenu s'il doit pour ce faire révéler les détails intimes de sa vie à plusieurs dizaines de millions d'individus de par le monde.

Quelles que soient les raisons ayant entouré ce revirement, accueillons avec plaisir l'engagement du gouvernement fédéral à instaurer d'ici

l'an 2000 ce que l'ancien ministre de la Justice d'alors, Allan Rock,

a qualifié de législation efficace et solide en matière de protection de la vie privée au sein des entreprises canadiennes. Cet engagement a reçu l'aval du Commissariat et des commissaires à la vie privée provinciaux, des défenseurs de la vie privée et, qui plus est, des membres du Comité consultatif sur l'autoroute électronique.

Les ministres fédéraux de l'Industrie et de la Justice ont publié un

document de consultation publique intitulé *La protection des renseignements personnels : pour une économie et une société de l'information au*

Canada, lequel invitait les réactions de la population canadienne. Ces ministères examinent actuellement les commentaires reçus (dont le

nôtre, expliqué à la page 12), lesquels seront reflétés dans un projet de loi dont le dépôt est prévu pour octobre 1998.

Il s'agit là, sans nulle exagération, de l'événement canadien le plus

marquant en matière de vie privée depuis la publication par le gouvernement du rapport *L'ordonnateur et la vie privée*, en 1971 (lequel avait mené à la Partie IV de la *Loi canadienne sur les droits de la personne*,

toute première protection de la vie privée du corpus juridique

canadien). S'il répond à la promesse de M. Rock, le futur projet de

loi placera le Canada à l'avant-plan des pays défenseurs de la vie privée. Sinon, les exceptions, exclusions et autres échappatoires d'un projet de loi faible en feront un désastre, surtout s'il ne prévoit pas de recours

indépendant et efficace.

Mon Commissariat vit donc en ce moment une grande (bien que

fébrile) espérance. Les puissants groupes de pression qui ont déjà

commencé à se porter à la défense de certains intérêts du secteur privé n'échappent pas à notre attention, et leurs pouvoirs nous inspirent un respect qu'il nous coûte d'avouer.

Quant à la surveillance de nos moindres faits et gestes, ce qui n'était qu'une lointaine tendance est devenue une réalité de plus en plus présente. Pas un jour ne se passe sans que nous n'apprenions la présence de caméras dans nos communautés, qui surveillent de leur sinistre objectif nos rues, nos commerces et nos bureaux. Bien que ces caméras soient officiellement chargées d'assurer notre sécurité, raison que nous acceptons parfois, c'est rarement le cas : que dire par exemple de ce propriétaire de bar qui souhaite filmer la mauvaise conduite de certains de ses clients?

L'omniprésence de ces caméras annonce la disparition de notre respect des droits individuels : il semble en effet plus facile et rapide d'espionner tous les clients et de réduire ainsi le plaisir qu'ils se promettaient de leur sortie que d'accepter la responsabilité d'assurer une ambiance civilisée en refusant la présence d'individus indésirables. Mais pire encore, nous acceptons sans broncher une telle surveillance! Nous voulons une sécurité à toute épreuve, et nous n'avons rien à cacher, n'est-ce pas? Alors, abriquons toute notion de liberté individuelle!

Changement de paysage

Mon septennat m'a fait changer mon fusil d'épaule sur un point majeur : la meilleure façon de nous protéger. En effet, alors que mon premier rapport annuel repoussait un renforcement des lois sur la vie privée au profit de mécanismes volontaires, j'ai dû vite déchanter. En 1995, je reconnaissais, à contrecoeur, avoir progressivement constaté l'inefficacité de tels mécanismes, et j'encourageais le gouvernement fédéral et les provinces à suivre l'exemple québécois et à légiférer en matière de protection de la vie privée au sein des entreprises canadiennes.

La piètre réaction de ces entreprises est en partie responsable de mon changement, motivé également par l'accroissement des échanges de données entre les gouvernements et le secteur privé, la privatisation d'activités gouvernementales (et la perte de protection de la vie privée en découlant), et l'apparition d'une législation européenne sur les renseignements personnels qui pourrait bien empêcher tout transfert de ces derniers vers des pays, tel le Canada, ne leur garantissant pas de protection adéquate.

Puisque ce rapport annuel fait le pont entre la fin de mon mandat de sept ans et sa prolongation de vingt-quatre mois, je profite de l'occasion pour remercier le Parlement de me permettre de m'attaquer à deux questions pressantes : la mise en place d'une loi efficace sur la protection de la vie privée au sein des entreprises canadiennes, et la protection de nos dossiers médicaux dans le cadre d'une éventuelle infrastructure des renseignements de santé. Je reviendrai sur ces deux enjeux plus bas.

Ces sept années ont vu la continuation de bien des changements pour nos renseignements et tous les risques qui en découlent. Les prophéties d'alors se sont toutes avérées exactes, et les renseignements personnels de millions d'individus font l'objet de collectes, de manipulations, d'analyses, d'achats, de ventes, et d'abus infiniment plus fréquents et rapides que la technologie ne le permettrait il y a sept ans.

L'Internet, qui est le plus massif et, potentiellement, le plus libérateur des moyens de communication de l'histoire est arrivé à maturité : des millions de gens s'y branchent chaque année, le poussant à devenir aussi populaire que le téléphone, qu'il pourrait d'ailleurs finir par supplanter pour l'ensemble des transactions commerciales et des communications personnelles de la planète.

Mais l'Internet a aussi suscité de nouveaux problèmes : atteintes à la vie privée, à la décence et à la vérité (sans parler de notre sécurité personnelle). Ces problèmes poussent la société, et plus particulièrement les élus, à vouloir contrôler l'Internet. Mais ce qui est louable dans certains cas, telle l'élimination de la vente de matériel pornographique, devient répréhensible dans d'autres. Le meilleur exemple en est probablement la volonté de notre gouvernement de contrôler la disponibilité et l'utilisation des moyens de chiffrement, alors qu'il s'agit là de la meilleure technologie à l'heure actuelle pour garantir la sécurité et la confidentialité des transactions commerciales électroniques. De telles mesures pourraient bien créer une telle inhibition parmi les usagers qu'elles pourraient étouffer la majeure partie de la valeur de ce merveilleux et flexible médium planétaire qu'est l'Internet.

Table des matières

Cent fois sur le métier	1
Une loi sur la vie privée applicable au secteur privé	12
Protection des renseignements personnels et santé	19
Direction des enquêtes	22
Cas	23
Demandes de renseignements	49
Tableaux et diagrammes	50
Fenêtre élargie sur les questions de vie privée :	60
Gestion des politiques et recherche	60
Le rêve de tout marcaticien...cauchemar pour la vie privée?	62
Peut-on garder un secret ?	65
La carotte devant l'âne -	68
Politique sur les réseaux électroniques	68
Internet - toujours pas de vie privée	71
Une expérience qui porte fruits	76
Loi sur la banque de données sur l'ADN	80
et le système judiciaire criminel	80
Calendrier législatif	82
Mises à jour	87
Les annuaires téléphoniques, liste électorale permanente, les ententes de partage gagnent en visibilité	94
Avis de coupages de données	94
Programme canadien de prêts aux étudiants au fichier des employés gouvernementaux, Programme de prestations d'invalidité de l'Alberta au Régime de pensions du Canada, la Sécurité de la vieillesse et les avis de décès du Régime de pensions du Québec	99
Devant les tribunaux	102
Cas, la Charte - attente raisonnable de respect de vie privée	102
Protection de la vie privée au Canada	111
Gestion intégrée	114
Organigramme	117



Commissaire
à la protection de
la vie privée du Canada
Privacy
Commissioner
of Canada

juillet 1998

L'honorable Gilbert Parent
Président
Chambre des communes
Ottawa

Monsieur,

J'ai l'honneur de soumettre mon rapport annuel au Parlement.
Le rapport couvre la période allant du 1^{er} avril 1997 au 31 mars 1998.

Veillez agréer, Monsieur, l'expression de mes sentiments respectueux.

Le Commissaire,

Bruce Phillips
Bruce Phillips



Commissaire
à la protection de
la vie privée du Canada
Privacy
Commissioner
of Canada

juillet 1998

L'honorable Gildas L. Molgat
Président
Sénat
Ottawa

Monsieur,

J'ai l'honneur de soumettre mon rapport annuel au Parlement.
Le rapport couvre la période allant du 1^{er} avril 1997 au 31 mars 1998.
Veuillez agréer, Monsieur, l'expression de mes sentiments respectueux.

Le Commissaire,

Bruce Phillips
Bruce Phillips

Le Commissaire à la protection de la vie privée du Canada

112, rue Kent

Ottawa (Ontario)

K1A 1H3

(613) 995-2410, 1-800-267-0441

Téléc. (613) 947-6850

ATS (613) 992-9190

© Ministre des Travaux publics et Services gouvernementaux Canada 1998

N° de cat. IP 30-1/1998

ISBN 0-662-63685-6

Cette publication est offerte sur cassette et sur disquette informatique.

Nous sommes accessibles sur le réseau Internet à : <http://infoweb.magi.com/~privcan/>

rapport annuel 1997-1998

Commissionnaire à la protection de la vie privée



rapport annuel 1997-1998

Commission de la protection de la vie privée



